整数的性质

朱思良編著

上海教育出版社

一九五八年·上海

整　数　的　性　質

朱思良編著

*

上海教育出版社出版

（上海永福路123号）

上海市書刊出版业营业許可証出090号

大东集成联合厂印刷　新华書店上海发行所总經售

*

开本：850×1168 . 1/32　印張：6 9/16　字数：173,000

1958年12月第1版　1958年12月第1次印刷

印数：1—13,000本

統一書号：7150・206

定　　价：(7)0.70元

序

整数是“数”的基础，只有在了解了整数的一系列性质后，才能研究其他数的性质，从而可以把研究的結果用到数学各个学科中去。事实上，即使在中学数学的范圍內，我們也到处可以遇到涉及整数性质的問題。

专門研究整数的性质，是属于“整数論”的任务。本書虽然也是討論整数的性质，但与作为学科的“整数論”有些不同。它的特点是：对于在中学数学范圍中遇到的整数性质問題加以詳細且深入的討論。另外，对于一些虽是比較深奥，可是很有趣，或在今后进一步研究整数理論时很有用的，同时又能为具有中学数学程度的同志所能接受的若干問題，也深入淺出地作了介紹。

这本書共分九章。前四章討論的內容是关于数的整除性理論。在这一部分里，我們将不仅看到“数的整除性”是研究整数理論的基础；而且还把从前有关这方面的一些直观的、零星的知識，在理論、方法、系統上加强了。

第五、第九两章討論的內容属于同余的理論。“同余”是整数理論中最重要的內容。因限于本書的性质，对于“同余”不作过深的探討。但是即使这样，我們还是可以看到这个內容是多么的丰富。这些內容扩大了我們对整数的認識。同时我們也可以看到这些理論在中学数学教学实踐中的应用。例如两整数相除求余数問題、运算正确性的檢驗等等。

第六章的內容是討論“一个整值多項式被某自然数整除的問題”。这类問題我們可以从各种数学杂志难題征解栏里、中学数学竞賽題中看到。对于这类問題有些青年学生表現出特殊的爱好。

第七章是討論“不定方程的整数解”。这是一个用整数理論来解决代数問題的例子。里面討論得比較詳細、深入的是“整系数两元一次方程的整数解”問題。

第八章是討論“連分数”。在进一步研究整数理論的时候，經常要用到連分数。既然这样，这里介紹了連分数的概念和性质以及它的初步应用。当然，更加深入的介紹不是本書的任务。

这本書所适合的讀者首先是：中学数学教师和正在师范学院数学系科学习的未来的中学教师。这本書对于这些同志說来，一方面对于中学数学各科中与整数有关的問題可以得到全面、系統而且比較深入的了解，同时也获得了足够的知識，使今后能順利地进一步研究整数的理論。从后一种意义上来說，这本書也就是研究“整数論”的跳板，也可以說是“整数論初步”。

作者的数学修养不够，表述能力也差，再說学习数論的时間也不长，所以这本書一定会存在不少缺点和錯誤。欢迎同志們批評、指教，使以后有机会可加以改进。

朱思良于1958年5月

目　录

前　　言

整数，誰都知道是包括着正整数（自然数）1，2，3，……，零以及負整数 $-1, -2, -3, \cdots\cdots$.

要熟悉这里所写的整数的性质，无疑地应該先掌握关于整数四則运算的性质.現在仅就下面經常会用到的两数相除的概念，复习一下.

定理　对于任意的整数 a、b $(b\neq0)$，一定存在也只存在一对整数 q、r，使

$$a=bq+r. \quad (0\leqslant r<|b|) \tag{1}$$

証明　先証明 $b>0$ 的时候，定理成立.

因为可以找到一个整数 q，使 bq 不大于 a，而 $b(q+1)$ 却大于 a. 設 $a-bq=r$，那末 $a=bq+r$，这里 $0\leqslant r<b$.

$r\geqslant0$ 是很明显的. 至于为什么 $r<b$ 呢？因为，如果 $r\geqslant b$，設 $r=b+r'$（当然 $r'\geqslant0$）. 于是 $a=bq+r=bq+b+r'=b(q+1)+r'$，也就是說，$a\geqslant b(q+1)$. 这就与 $a<b(q+1)$ 矛盾. 所以 $r<b$. 其次，証明符合这样条件的一对整数 q、r 是唯一的.如果另有一对整数 q_1 和 r_1，使 $a=bq_1+r_1$ $(0\leqslant r_1<b)$，那末 $bq+r=bq_1+r_1$. 即 $b(q-q_1)=r_1-r$. 如果 $q\neq q_1$，而 $q-q_1$ 显然是一个非零整数. 这样，等式左边的絕对值就不会小于 b，然而右边 r_1-r 的絕对值却小于 b. 于是等式一定不能成立. 如果 $q=q_1$，等式左边等于零，于是只当 $r=r_1$ 的时候，这个等式才能成立.所以說，一对整数 q、r 是唯一存在的.

下面再証明当 $b<0$ 的时候定理也成立.

因为对于 a、$|b|$，一定存在一对整数 q'、r，使

$$a=|b|q'+r, \quad (0\leqslant r<|b|)$$

即 $$a=b(-q')+r.$$

設 $-q'=q$，就有 $a=bq+r$. 因为整数对 q'、r 是唯一地存在的，所以 q、r 也是唯一地存在的．到这里，定理被証实了．

如果 $r=0$，我們就說 a 能被 b 整除，或 b 能整除 a. 以后我們用記号 $a \vdots b$ 来表示 a 能被 b 整除．

如果 $a \vdots b$，我們也說 a 是 b 的倍数；b 是 a 的約数．当 $a \vdots b$ 而 m 是整数的时候，下面的一些性质是讀者已經知道了的．

1．如果 $a \div b=c$，那末

(1) $$am \div b=cm;$$

(2) $$\frac{a}{m} \div b=\frac{c}{m} \quad (\text{如果 } a \vdots m);$$

(3) $$a \div bm=\frac{c}{m} \quad (\text{如果 } c \vdots m);$$

(4) $$a \div \frac{b}{m}=cm \quad (\text{如果 } b \vdots m);$$

(5) $$am \div bm=c;$$

(6) $$\frac{a}{m} \div \frac{b}{m}=c \quad (\text{如果 } a \vdots m,\ b \vdots m).$$

2．倍数的基本性质：

(1) 如果 $a \vdots b$, $b \vdots c$，那末 $a \vdots c$.

証明 已知 $a \vdots b$，一定存在整数 q，使 $a=bq$. 已知 $b \vdots c$，一定也存在整数 q'，使 $b=cq'$. 所以 $a=bq=(cq')q=c(q'q)$. 而 $q'q$ 是整数，所以 $a \vdots c$.

(2) 如果 $a_1 \vdots b$, $a_2 \vdots b$，那末 $a_1 \pm a_2 \vdots b$.

証明 $\because$ $a_1 \vdots b$, $a_2 \vdots b$，一定存在两整数 q_1 和 q_2，使 $a_1=bq_1$, $a_2=bq_2$. $\therefore$ $a_1 \pm a_2=bq_1 \pm bq_2=b(q_1 \pm q_2)$. $\because$ $q_1 \pm q_2$ 是整数，$\therefore$ $a_1 \pm a_2 \vdots b$.

这个定理可以加以推广：

如果整数 $a_1, a_2, \cdots\cdots, a_n$ 都能被 b 整除，那末

$$(a_1+a_2+\cdots\cdots+a_n) \vdots b. \text{（証明从略）}$$

(3) 如果 $a \vdots b$，且 p 是整数，那末 $pa \vdots b$.

証明 如果 $p=0$，这个結論显然是成立的；

如果 $p>0$，因为 $a \vdots b$，而 $pa=\underbrace{a+\cdots\cdots+a}_{p\text{个}}$，那末根据(2)，$pa \vdots b$；

如果 $p<0$，設 $p'=-p$（当然 $p'>0$），那末 $p'a \vdots b$. 設 $p'a=bq$，于是 $pa=(-p')a=-p'a=-bq=b(-q)$. 因为 $-q$ 是整数，也就是說，$pa \vdots b$.

引用(2)更可以把这条定理加以推广：

如果整数 $a_1, a_2, \cdots\cdots, a_n$ 都能被 b 整除，又 $p_1, p_2, \cdots\cdots, p_n$ 是任意的整数，那末 $p_1a_1+p_2a_2+\cdots\cdots+p_na_n \vdots b$.

例 整数 21, 14, 56 都能被 7 整除，任意取三个整数 2, 3, -1，很容易看到 $21\cdot2+14\cdot3+56\cdot(-1)=28 \vdots 7$.

第一章 最大公約数及最小公倍数

从第一章到第四章的內容是属于数的整除性理論，而第一章的內容也就是整除性理論的基础．根据整数相除的概念，在这一章里我們要建立关于最大公約数和最小公倍数的概念，从而比較詳尽且深刻地探討它們的性質．掌握了几个数的最大公約数和最小公倍数的性質，就可以用来指导求几个数的最大公約数和最小公倍数了．

§1 公約数公倍数的意义

如果 $a_1, a_2, \cdots\cdots, a_n$ 及 p 都是整数，且 $a_1 \vdots p, a_2 \vdots p, \cdots\cdots, a_n \vdots p$，那末 p 就叫做 $a_1, a_2, \cdots\cdots, a_n$ 的公約数．

因为每一个数的約数的个数是有限的，所以几个数的公約数的个数也是有限的．

几个数的公約数中数值最大的一个，叫做这几个数的最大公約数．如果 d 是 $a_1, a_2, \cdots\cdots, a_n$ 这 n 个数的最大公約数，可以記作：

$$(a_1, a_2, \cdots\cdots, a_n)=d.$$

几个数的最大公約数一定存在而且是唯一的．这个論断很容易被証实：

譬如对 $a_1, a_2, \cdots\cdots, a_n$ 这 n 个数，可以知道它們存在公約数（最容易指出的就是 ± 1），而且公約数的个数是有限个．設这有限个公約数是 $d_1, d_2, \cdots\cdots, d_m$，而 d 是 $d_1, d_2, \cdots\cdots, d_m$ 中最大的一个，記作 $max[d_1, d_2, \cdots\cdots, d_m]=d$．根据定义，这个数 d 就是 $a_1, a_2, \cdots\cdots, a_n$ 的最大公約数．这就証明了 $a_1, a_2, \cdots\cdots, a_n$ 的最大公約数是存在的．至于最大公約数的唯一性更容易証明：設 $d'=(a_1, a_2, \cdots\cdots, a_n)$，且 $d'\neq d$，按照几个数的最大公約数的意义，那末 $d'\geqslant d$．但是已知 $d=(a_1, a_2, \cdots\cdots, a_n)$，那末 $d\geqslant d'$．很明显，只当 $d=d'$ 的时候，这两个結論間才沒有矛盾．

当 $(a, b)=1$ 的时候，我們把 a, b 叫做两个互質的数．同理，如果 $(a_1, a_2, \cdots\cdots, a_n)=1$，$a_1, a_2, \cdots\cdots, a_n$ 这 n 个数就叫做互質的数．

如果 $a_1, a_2, \cdots\cdots, a_n$ 中每一个数都与其中的另一个数互質，那末，我們把 $a_1, a_2, \cdots\cdots, a_n$ 这 n 个数叫做两两互質．

我們不能把多个互質的数与多个数两两互質这两个概念混淆起来．如果 $a_1, a_2, \cdots\cdots, a_n$ 两两互質，那末 $(a_1, a_2, \cdots\cdots, a_n)=1$；反过来却不成立，就是如果 $(a_1, a_2, \cdots\cdots, a_n)=1$，$a_1, a_2, \cdots\cdots, a_n$ 这几个数不一定两两互質．

例如，$(6, 10, 15)=1$，但 6，10，15 并不两两互質．当然也有这种情形，例如，24，17，11，5 这四个数不仅是互質，而且是两两互質的．

下面我們来給公倍数下定义：

如果 $m \vdots a_1, m \vdots a_2, \cdots\cdots, m \vdots a_n$，那末，$m$ 就叫做 $a_1, a_2, \cdots\cdots, a_n$ 这几个数的公倍数．

很明显，几个数的公倍数的个数是无限的．因为几个数的公倍数的

倍数还是这几个数的公倍数.

几个数的一切公倍数中的最小正数,叫做这些数的最小公倍数.

如果 m 是 $a_1, a_2, \cdots\cdots, a_n$的最小公倍数,可以記作:

$$[a_1, a_2, \cdots\cdots, a_n]=m.$$

几个数的最小公倍数一定存在且是唯一的. 这个論断也很容易被証实:

譬如对 $a_1, a_2, \cdots\cdots, a_n$ 这 n 个数, 可以知道它們存在公倍数(最容易指出的一个就是乘积 $\pm a_1a_2\cdots\cdots a_n$), 并且它的个数是无限的. 下面的一个事实是够明显的:在一些自然数中(不論它的个数是有限的还是无限的),总可以找到一个最小的数.

根据这一点, 也就是說可以在无限个正的公倍数中找到一个最小的,設为 m, 那末,$[a_1, a_2, \cdots\cdots, a_n]=m$.

这就証明了 $a_1, a_2, \cdots\cdots, a_n$ 的最小公倍数是存在的. 关于最小公倍数的唯一性的証明如下: 設$m'=[a_1, a_2, \cdots\cdots, a_n]$, 且 $m'\neq m$. 按照几个数的最小公倍数的意义, 那末, $m'\leqslant m$. 但是已經知道 $m=[a_1,a_2,\cdots\cdots,a_n]$, 就是說, $m\leqslant m'$. 很明显, 只当 $m=m'$ 的时候, 結論才合理.

在进入下一节的討論之前,預先作一个声明:因为$a_1, a_2, \cdots\cdots, a_n$ 的公約数(或公倍数)也就是$|a_1|, |a_2|, \cdots\cdots, |a_n|$ 的公約数(或公倍数),反过来也成立,特别有

$$(a_1, a_2, \cdots\cdots, a_n)=(|a_1|, |a_2|, \cdots\cdots, |a_n|);$$

及 $[a_1, a_2, \cdots\cdots, a_n]=[|a_1|, |a_2|, \cdots\cdots, |a_n|]$.

同时,如果数 s 是 $a_1, a_2, \cdots\cdots, a_n$ 的公約数(或公倍数),那末$|s|$也就是 $a_1, a_2, \cdots\cdots, a_n$ 的公約数(或公倍数),反过来也成立. 因为这样,为了書写的簡单明了起見,在本章中,从下一节开始,字母所表示的数,除特别加以声明外,一般只限于正整数.

§2 最大公約数的性质

下面1到6討論的是关于两个数的最大公約数的一些性質.

1. 如果 $a \vdots b$, 那末 b 的約数就是 a、b 的公約数.反过来也成立.

証明 設 p 是 b 的約数, $b \vdots p$; 因为 $a \vdots b$, 所以 $a \vdots p$. 这就証明了 p 是 a、b 的公約数. 反过来,如果某数是 a、b 的公約数, 当然这个数一定是 b 的約数.

推論 如果 $a \vdots b$, 那末 $(a, b)=b$.

2. 如果 b 不能整除 a, 且 $a>b$, 就是說, $a=bq+r$, 那末 a、b 的所有公約数一定是 b、r 的公約数.反过来也成立.

証明 設 m 是 a、b 的公約数, 就是 $a \vdots m$, $b \vdots m$. 如果 q 是整数,当然 $bq \vdots m$. 因为 $a-bq=r$, 根据倍数的基本性質,那末 $r \vdots m$. 就是 m 也是 b、r 的公約数. 上面就証明了 a、b 的所有公約数一定是 b、r 的公約数. 同理可証得, b、r 的所有公約数也一定是 a、b 的公約数.

推論 如果 $a=bq+r$, 那末 $(a, b)=(b, r)$.

証明 設 $(a, b)=d$, 根据 2 知道 d 一定是 b、r 的公約数. 設 $(b,r)=d'$,当然 d' 也是 a、b 的公約数. 如果 $d'>d$,就是 d' 比 a、b 的最大公約数还大,显然是不合理的. 如果 $d'<d$, 就是 d 比 b、r 的最大公約数还大,显然也不合理. 所以 $d'=d$. 也就是說,$(a, b)=(b, r)$.

从这个推論更可推出以下两个特殊情形:

$$(a+b, b)=(a, b); \quad (a-b, b)=(a, b).$$

3. 欧几里德除法(輾轉相除法):

設任意两个正整数 a、b, 且 $a>b$, 用 b 去除 a, 得 $a=bq_1+r_1$ $(r_1<b)$. 如果 $r_1 \neq 0$, 我們用 r_1 去除 b, 于是得 $b=r_1q_2+r_2 (r_2<r_1)$. 如果 $r_2 \neq 0$, 我們再用 r_2 去除 r_1, 得 $r_1=r_2q_3+r_3$ $(r_3<r_2)$. 如果 $r_3 \neq 0$, 我們用 r_3 去除 r_2, 这样繼續地进行下去. 然而我們可以断定这个过程不会是无穷尽的, 事实上一定能找到 $r_n=0$. 因为这里所得到的一連串整数 b、r_1、r_2、r_3、…… 有着下列关系:

$$b>r_1>r_2>r_3>\cdots\cdots.$$

很明显，满足这样关系的整数不可能是无限个．这就說明了我們一定能得到等式 $r_{n-2}=r_{n-1}q_n+r_n$，而 $r_n=0$。

定理 对两个自然数 a、b（設 $a>b$），根据以上所述一定存在下面一系列的等式：

$$a=bq_1+r_1,\quad (0<r_1<b) \tag{1}$$

$$b=r_1q_2+r_2,\quad (0<r_2<r_1) \tag{2}$$

$$r_1=r_2q_3+r_3,\quad (0<r_3<r_2) \tag{3}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1},\quad (0<r_{n-1}<r_{n-2}) \tag{n-1}$$

$$r_{n-2}=r_{n-1}q_n+r_n,\quad (r_n=0) \tag{n}$$

那末，$(a,\ b)=r_{n-1}$。

証明 由等式(1)，得 $(a,\ b)=(b,\ r_1)$，

由等式(2)，得 $(b,\ r_1)=(r_1,\ r_2)$，

由等式(3)，得 $(r_1,\ r_2)=(r_2,\ r_3)$，

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$

由等式$(n-1)$，得 $(r_{n-3},\ r_{n-2})=(r_{n-2},\ r_{n-1})$，

由等式(n)，得 $(r_{n-2},\ r_{n-1})=r_{n-1}$. $(\because\ r_{n-2}\ \vdots\ r_{n-1}.)$

于是$(a,\ b)=(b,\ r_1)=(r_1,\ r_2)=\cdots\cdots=(r_{n-2},\ r_{n-1})=r_{n-1}$.

4．如果 a，b，δ 是任意三个正整数，那末$(a,\ b)\ \vdots\ \delta$ 的充分而且必要条件是：$a\ \vdots\ \delta$，$b\ \vdots\ \delta$.

証明 关于条件的充分性：

我們不妨假定 $a>b$，且設$(a,\ b)=d$，根据性質 3，可以知道，下面一系列等式是成立的：

$$a=bq_1+r_1, \tag{1}$$

$$b=r_1q_2+r_2, \tag{2}$$

$$\cdots\cdots\cdots\cdots,$$

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}, \tag{n-1}$$

$$r_{n-2}=r_{n-1}q_n+r_n. \quad (r_n=0) \tag{n}$$

根据性质 2，因为 $a \vdots \delta$, $b \vdots \delta$, 由等式(1)，得到 $r_1 \vdots \delta$. 同理，由等式(2)可得到 $r_2 \vdots \delta$. 这样繼續下去当然可以推得，$r_{n-3} \vdots \delta$, $r_{n-2} \vdots \delta$. 再从等式$(n-1)$ 可以得到 $r_{n-1} \vdots \delta$. 性質 3 告訴我們 $(a, b)=r_{n-1}$，就是說 $d=r_{n-1}$. 于是就証明了 $d \vdots \delta$.

至于条件的必要性成立的理由是簡单的：

如果$(a, b)=d \vdots \delta$, 很明显，因为 $a \vdots d$, 而 $d \vdots \delta$, 所以 $a \vdots \delta$, 同理可得 $b \vdots \delta$.

5. 如果$(a, b)=d$, 那末$(ma, mb)=md$.

証明 因为 $a \vdots d$, $b \vdots d$, 所以 $ma \vdots md$, $mb \vdots md$. 就是說 md 是 ma 和 mb 的公約数.

設 $(ma, mb)=d'>md$, 由性質 4，可以知道 $d' \vdots md$. 因为 $md \vdots m$, 所以 $d' \vdots m$. 設 $d'=mq$, 因为 $ma \vdots d'$, $mb \vdots d'$, 也就是 $ma \vdots mq$, $mb \vdots mq$. 于是得到 $a \vdots q$, $b \vdots q$. 所以 q 是 a、b 的公約数. 然而，因为 $d'>md$, 就是$\dfrac{d'}{m}=q>d$. 因此 q 不可能是 a、b 的公約数(两个数的公約数当然不会比它們的最大公約数还大)。这就是說，假設 $d'>md$ 是不成立的，而 $(ma, mb)=md$.

推論 如果$(a, b)=d$, 而 $a \vdots \delta$, $b \vdots \delta$, 那末

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)=\frac{d}{\delta}.$$

証明 因为$\left(\dfrac{a}{\delta}, \dfrac{b}{\delta}\right)\cdot\delta=\left(\dfrac{a}{\delta}\cdot\delta, \dfrac{b}{\delta}\cdot\delta\right)=(a, b)=d$,所以

$$\left(\frac{a}{\delta}, \frac{b}{\delta}\right)=\frac{d}{\delta}.$$

6. 如果 a, b, d 是任意三个正整数，那末$(a, b)=d$ 的充分而且必要条件是：

$$\left(\frac{a}{d}, \frac{b}{d}\right)=1.$$

証明　关于条件的必要性：

如果$(a, b)=d$，于是$a \vdots d$，$b \vdots d$；这样，由性质5的推論可以知道

$$\left(\frac{a}{d}, \frac{b}{d}\right)=\frac{d}{d}=1.$$

关于条件的充分性：

由性质5可以知道，因为$\left(\frac{a}{d}, \frac{b}{d}\right)=1$ 得到$\left(\frac{a}{d}\cdot d, \frac{b}{d}\cdot d\right)=1\cdot d.$ 就是$(a, b)=d.$

下面从7到10討論的是关于多个数的最大公約数的一些性质．

7．設$(a_1, a_2)=d_1$，$(d_1, a_3)=d_2$，$(d_2, a_4)=d_3$，………，$(d_{n-3}, a_{n-1})=d_{n-2}$，$(d_{n-2}, a_n)=d_{n-1}$，那末

$$(a_1, a_2, \cdots\cdots, a_n)=d_{n-1}.$$

証明　我們說d_{n-1}是$a_1, a_2, \cdots\cdots, a_n$的公約数的理由如下：由已知条件知道$a_1 \vdots d_1$，$a_2 \vdots d_1$，$a_3 \vdots d_2$，$a_4 \vdots d_3$，……，$a_{n-1} \vdots d_{n-2}$，$a_n \vdots d_{n-1}$；又因为$d_1 \vdots d_2$，$d_2 \vdots d_3$，……，$d_{n-3} \vdots d_{n-2}$，$d_{n-2} \vdots d_{n-1}$，这样，容易看到$d_{n-1}$是$d_1, d_2, \cdots\cdots, d_{n-2}, d_{n-1}$的公約数．而$d_1$、$d_2$、……、$d_{n-2}$、$d_{n-1}$又分别是$a_2$、$a_3$、……、$a_{n-1}$、$a_n$的約数（$d_1$既是$a_2$的約数也是$a_1$的約数）．所以$d_{n-1}$是$a_1, a_2, \cdots\cdots, a_n$諸数的公約数，接下来我們要証明$d_{n-1}$是它們的最大公約数：

設$(a_1, a_2, \cdots\cdots, a_n)=d_k>d_{n-1}$，当然

$$a_1 \vdots d_k, \ a_2 \vdots d_k, \ \cdots\cdots, \ a_n \vdots d_k.$$

已知$(a_1, a_2)=d_1$，而这里又知道$a_1 \vdots d_k$，$a_2 \vdots d_k$，所以根据性质4得：

$$d_1 \vdots d_k;$$

已知$(d_1, a_3)=d_2$，而这里又知$d_1 \vdots d_k$，$a_3 \vdots d_k$，所以得：

$$d_2 \vdots d_k;$$

………………………………………；

已知$(d_{n-2}, a_n)=d_{n-1}$，而又知$d_{n-2} \vdots d_k$，$a_n \vdots d_k$，所以得：

$$d_{n-1} \vdots d_k.$$

很明显，如果 $d_{n-1} \vdots d_k$，那末 $d_{n-1} \geqslant d_k$. 这就与假設 $d_k > d_{n-1}$ 矛盾. 所以 $(a_1, a_2, \cdots\cdots, a_n) = d_{n-1}$.

推論 1 如果 $(a_1, a_2, \cdots\cdots, a_k) = d$，那末

$$(a_1, a_2, \cdots\cdots, a_k, a_{k+1}, \cdots\cdots, a_n) = (d, a_{k+1}, \cdots\cdots, a_n).$$

証明 設 $(a_1, a_2) = d_1$，$(d_1, a_3) = d_2$，$\cdots\cdots$，$(d_{k-2}, a_k) = d_{k-1}$，$\cdots\cdots$，$(d_{n-2}, a_n) = d_{n-1}$，那末 $(a_1, a_2, \cdots\cdots, a_n) = d_{n-1}$. 这里还可以看到 $(a_1, a_2, \cdots\cdots, a_k) = d_{k-1}$，而 $d_{k-1} = d$.

由 $(d_{k-1}, a_{k+1}) = d_k$，$(d_k, a_{k+2}) = d_{k+1}$，$\cdots\cdots$，$(d_{n-2}, a_n) = d_{n-1}$，可以知道 $(d_{k-1}, a_{k+1}, \cdots\cdots, a_n) = d_{n-1}$. 就是 $(d, a_{k+1}, \cdots\cdots, a_n) = d_{n-1}$.

这就証明了 $(a_1, a_2, \cdots\cdots, a_n) = (d, a_{k+1}, \cdots\cdots, a_n)$.

推論 2 如果 $(a_1, a_2, \cdots\cdots, a_k) = d$，$(a_{k+1}, \cdots\cdots, a_n) = d'$，

那末 $(a_1, a_2, \cdots\cdots, a_n) = (d, d')$.

証明 因为 $(a_1, a_2, \cdots\cdots, a_n) = (d, a_{k+1}, \cdots\cdots, a_n) = (a_{k+1}, \cdots\cdots, a_n, d)$，已知 $(a_{k+1}, \cdots\cdots, a_n) = d'$，由推論 1 可以知道 $(a_{k+1}, \cdots\cdots, a_n, d) = (d', d)$. 所以 $(a_1, a_2, \cdots\cdots, a_n) = (d, d')$.

8. 如果 $a_1, a_2, \cdots\cdots, a_n, \delta$ 是任意正整数，$(a_1, a_2, \cdots\cdots, a_n) \vdots \delta$ 的充分而且必要条件是：$a_1 \vdots \delta$，$a_2 \vdots \delta$，$\cdots\cdots$，$a_n \vdots \delta$.

証明 关于条件的充分性：

設 $(a_1, a_2) = d_1$，$(d_1, a_3) = d_2$，$\cdots\cdots$，$(d_{n-3}, a_{n-1}) = d_{n-2}$，$(d_{n-2}, a_n) = d_{n-1}$. 于是，得到 $(a_1, a_2, \cdots\cdots, a_n) = d_{n-1}$.

因为 $(a_1, a_2) = d_1$，而已知 $a_1 \vdots \delta$，$a_2 \vdots \delta$，所以 $d_1 \vdots \delta$；

因为 $(d_1, a_3) = d_2$，而已知 $d_1 \vdots \delta$，$a_3 \vdots \delta$，所以 $d_2 \vdots \delta$；

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$；

因为 $(d_{n-2}, a_n) = d_{n-1}$，而已知 $d_{n-2} \vdots \delta$，$a_n \vdots \delta$，所以 $d_{n-1} \vdots \delta$.

这就証明了 $(a_1, a_2, \cdots\cdots, a_n) \vdots \delta$.

关于条件的必要性的証明极容易，这里从略.

9. 如果 $(a_1, a_2, \cdots\cdots, a_n) = d$，那末 $(ma_1, ma_2, \cdots\cdots, ma_n) = md$.

証明 由 $a_1 \vdots d$，$a_2 \vdots d$，$\cdots\cdots$，$a_n \vdots d$，可以得到 $ma_1 \vdots md$，

$ma_2 \vdots md, \cdots\cdots, ma_n \vdots md$. 于是說，$md$ 是 $ma_1, ma_2, \cdots\cdots, ma_n$ 的公約数，然后証明 md 是 $ma_1, ma_2, \cdots\cdots, ma_n$ 的最大公約数：.

設$(ma_1, ma_2, \cdots\cdots, ma_n)=d'>md$，当然 $d' \vdots md$. 根据性质 8，$d' \vdots m$. 設 $d'=mq$，于是得 $mq \vdots md$，也就是 $q \vdots d$. 而且 $q>d$（$\because d'>md$）.

由假設得到 $ma_1 \vdots d', ma_2 \vdots d', \cdots\cdots, ma_n \vdots d'$，因为 $d'=mq$，就得到 $a_1 \vdots q, a_2 \vdots q, \cdots\cdots, a_n \vdots q$. 这样，因为 d 是 $a_1, a_2, \cdots\cdots, a_n$ 这几个数的最大公約数，而 q 是它們的公約数，公約数 q 怎么会大于最大公約数 d 呢？很明显，上面的假設不成立，也就是說，

$$(ma_1, ma_2, \cdots\cdots, ma_n)=md.$$

推論 如果 $a_1 \vdots \delta, a_2 \vdots \delta, \cdots\cdots, a_n \vdots \delta$，而 $(a_1, a_2, \cdots\cdots, a_n)=d$，那末，$\left(\frac{a_1}{\delta}, \frac{a_2}{\delta}, \cdots\cdots, \frac{a_n}{\delta}\right)=\frac{d}{\delta}$.

証明留給讀者.

10. 如果 $a_1, a_2, \cdots\cdots, a_n, d$ 是任意正整数，那末$(a_1, a_2, \cdots\cdots, a_n)=d$ 的充分而且必要条件是：

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots\cdots, \frac{a_n}{d}\right)=1.$$

証明留給讀者.

下面再討論关于互质的数的一些性质.

11. 如果$(a, b)=1$，那末$(ac, b)=(c, b)$.

証明 已知$(a, b)=1$，那末$(ac, bc)=c$.

如果$(ac, b)=d$，那末 $ac \vdots d, b \vdots d$. 因为 $b \vdots d$，所以 $bc \vdots d$. 也就是說，d 是 ac 和 bc 的公約数. 因为$(ac, bc)=c$，于是 $c \vdots d$. 所以 d 是 b 和 c 的公約数. 設$(b、c)=d'$，那末 $d' \vdots d$.

由所設知 $c \vdots d'$（当然 $ac \vdots d'$），$b \vdots d'$，也就是說，d' 是 ac 和 b 的公約数. 因为$(ac, b)=d$，我們就得到 $d \vdots d'$. 要使 $d' \vdots d$，$d \vdots d'$ 这两个关系同时成立，显然只当 $d=d'$ 的时候. 所以$(ac, b)=(c, b)$.

推論 1　如果$(a, b)=1$, $(c, b)=1$, 那末$(ac, b)=1$.

因为当$(a, b)=1$的时候，$(ac, b)=(c, b)$. 而已知$(c, b)=1$，所以$(ac, b)=1$.

推广：如果 $(a_1, b)=1$, $(a_2, b)=1$, ……, $(a_n, b)=1$, 那末$(a_1a_2\cdots\cdots a_n, b)=1$.

推論 2　与a和b都互質的数及与$a\cdot b$互質的数以全体而言是一致的.

証明：設$(c, a)=1$, $(c, b)=1$, 由推論 1 知道$(c, ab)=1$. 就是与a及b都互質的数也与ab互質，反过来，如果$(c, ab)=1$, 且$(c, a)=d>1$. 設$c=dq$, $a=dq'$, 那末$(c, ab)=(dq, dq'b)=d(q, q'b)>1$. 这就与所設$(c, ab)=1$矛盾. 所以說，如果$(c, ab)=1$, 那末$(c, a)=1$. 同理可証$(c, b)=1$. 这就証明了与乘积$ab$互質的数一定与$a$也与$b$互質.

推論 3　如果$(a, b)=1$, 而$ac \vdots b$, 那末$c \vdots b$.

証明　$\because$ $(a, b)=1$,　$\therefore$ $(ac, b)=(c, b)$.　$\because$ $ac \vdots b$, $\therefore$ $(ac, b)=b$. 也就是說，$(c, b)=b$, 所以$c \vdots b$.

12. 如果等式 $(a_i, b_j)=1$ 对于i在 1, 2, ……, m 和j在 1, 2, ……, n 中各任取一数时都成立，那末$(a_1a_2\cdots\cdots a_m, b_1b_2\cdots\cdots b_n)=1$.

証明　由所設可知：$(a_1, b_j)=1$, $(a_2, b_j)=1$, ……, $(a_m, b_j)=1$, 于是 $(a_1a_2\cdots\cdots a_m, b_j)=1$.

設 $a_1a_2\cdots\cdots a_m=M$, 于是 $(M, b_j)=1$, 也就是$(b_j, M)=1$. 这也就得到下面一些关系式：

$(b_1, M)=1$, $(b_2, M)=1$, ……, $(b_n, M)=1$. 因此$(b_1b_2\cdots\cdots b_n, M)=1$. 这就証明了$(b_1b_2\cdots\cdots b_n, a_1a_2\cdots\cdots a_m)=1$. 也就是$(a_1a_2\cdots\cdots a_m, b_1b_2\cdots\cdots b_n)=1$.

例　3, 5, 11, 15 中的每一个数与 4, 7, 13 中的每一个数都互質，所以說，$(3\cdot5\cdot11\cdot15,\ 4\cdot7\cdot13)=1$.

推論　如果$(a, b)=1$, 且m、n是任意两个自然数，那末

$$(a^m, b^n)=1.$$

証明 $\because$ $(a, b)=1$，而这里 $a_1=a_2=\cdots\cdots=a_m=a$，$b_1=b_2=\cdots\cdots=b_n=b$. 于是 $a_1a_2\cdots\cdots a_m=a^m$，$b_1b_2\cdots\cdots b_n=b^n$. 所以$(a^m, b^n)=1$.

例如，$\because$ $(3, 4)=1$，$\therefore$ $(3^5, 4^8)=1$.

例 1 試証明$\sqrt[n]{A}$ (n, A 是正整数) 如果不是整数，那末便是无理数.

証明 如果$\sqrt[n]{A}=\dfrac{p}{q}$，这里 $q>1$，且$(p, q)=1$，那末 $A=\dfrac{p^n}{q^n}$. 因为$(p^n, q^n)=1$，且 $q^n>1$，所以說$\dfrac{p^n}{q^n}$不是整数. 但已知 A 是整数，所以等式 $A=\dfrac{p^n}{q^n}$显然不能成立，这个矛盾是由于假設$\sqrt[n]{A}$是分数而产生的. 所以說$\sqrt[n]{A}$如果不是整数便是无理数.

例 2 試証明 $\log_2 5$ 是无理数.

証明 如果 $\log_2 5=\dfrac{p}{q}$，这里 p、q 是正整数，且 $(p, q)=1$. 由对数定义可以得到 $2^{\frac{p}{q}}=5$. 也就是說，$2^p=5^q$. 然而 $(2, 5)=1$，所以对于任意值 p 和 q，$(2^p, 5^q)=1$. 这就是說，等式 $2^p=5^q$ 决不会成立. 因此，$\log_2 5$ 是无理数.

例 3 試証明整系数代数方程

$$x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0 \tag{1}$$

的有理根一定是整数根.

証明 如果方程(1)具有有理根 x，設 $x=\dfrac{p}{q}$，这里 $(|p|, q)=1$. 那末

$$\frac{p^n}{q^n}+a_1\cdot\frac{p^{n-1}}{q^{n-1}}+\cdots\cdots+a_{n-1}\cdot\frac{p}{q}+a_n=0.$$

也就是，$p^n+a_1p^{n-1}q+\cdots\cdots+a_{n-1}pq^{n-1}+a_nq^n=0$.

于是　　$p^n=-q[a_1p^{n-1}+a_2p^{n-2}q+\cdots\cdots+a_nq^{n-1}]=q\cdot M.$

所以 $p^n \vdots q$. 从而 $p \vdots q$. 因为$(|p|, q)=1$, 所以 $q=1$. 这就証明了如果方程(1)有有理根,該根一定是整数根.

由上面的推論还可以直接推出下面的性質:

$$(a^s, b^s)=(a, b)^s.$$

理由如下: 設$(a, b)=d$, 那末$\left(\frac{a}{d}, \frac{b}{d}\right)=1$. 于是得

$$\left(\frac{a^s}{d^s}, \frac{b^s}{d^s}\right)=1.$$

所以　　$(a^s, b^s)=d^s=(a, b)^s.$

上面的性質更可以推广到:

$$(a_1^s, a_2^s, \cdots\cdots, a_n^s)=(a_1, a_2, \cdots\cdots, a_n)^s.$$

理由如下: 設$(a_1, a_2)=d_1$, $(d_1, a_3)=d_2$, $\cdots\cdots$, $(d_{n-2}, a_n)=d_{n-1}$. 那末$(a_1, a_2, \cdots\cdots, a_n)=d_{n-1}$.

因为 $(a_1^s, a_2^s)=d_1^s$, $(d_1^s, a_3^s)=d_2^s$, $\cdots\cdots$, $(d_{n-2}^s, a_n^s)=d_{n-1}^s$. 所以$(a_1^s, a_2^s\cdots\cdots, a_n^s)=d_{n-1}^s$. 也就是,

$$(a_1^s, a_2^s, \cdots\cdots, a_n^s)=(a_1, a_2, \cdots\cdots, a_n)^s.$$

§3　最小公倍数的性質

从1到5先討論关于两个数的最小公倍数的一些性質.

1. 如果 $a \vdots b$, 那末 a 的倍数就是 a, b 的公倍数. 特別的有$[a, b]=a$.

因为理由很明显,証明就省略了.

2. 如果 M, a, b 是任意三个正整数, 那末 $M \vdots [a, b]$ 的充分而且必要条件是:

$$M \vdots a, \quad M \vdots b.$$

証明　先証明条件的充分性.

設 $[a, b]=\delta$, 如果 M 不能被 δ 整除, 那末一定存在一对整数 q、

r, 使 $M=q\delta+r\ (0<r<\delta)$.

已知 $M\vdots a$, 又 $\delta\vdots a$（当然 $q\delta\vdots a$）, 且 $r=M-q\delta$, 于是 $r\vdots a$. 同理可知 $r\vdots b$. 所以 r 是 a、b 的公倍数. 但 $r<\delta$, 这与 $[a, b]=\delta$ 矛盾. 因此 $M\vdots\delta$.

关于条件的必要性的証明是极容易的,这里省略了.

3. 如果 M, a, b 是任意三个正整数,那末 $[a, b]=\delta$ 的充分而且必要条件是:

$$\left(\frac{\delta}{a},\ \frac{\delta}{b}\right)=1.$$

証明 先証明条件的必要性:

設 $\delta=aq_1$, $\delta=bq_2$, 也就是 $\frac{\delta}{a}=q_1$, $\frac{\delta}{b}=q_2$. 如果 $(q_1, q_2)=d>1$, 設 $q_1=dp_1$, $q_2=dp_2$, 那末 $\frac{\delta}{a}=dp_1$, $\frac{\delta}{b}=dp_2$. 或 $\frac{\delta}{d}=ap_1$, $\frac{\delta}{d}=bp_2$.

設 $\frac{\delta}{d}=\delta'$, 因为 $d>1$, 所以 $\delta>\delta'$. 很容易看到 δ' 是 a, b 的公倍数,而这却与所設 $[a, b]=\delta$ 矛盾. 所以說, $(q_1, q_2)=d>1$ 是不合理的,也就是 $\left(\frac{\delta}{a},\ \frac{\delta}{b}\right)=1$.

关于条件的充分性的証明:

如果 $[a, b]\neq\delta$, 設 $[a, b]=\delta'<\delta$, 那末 $\left(\frac{\delta'}{a},\ \frac{\delta'}{b}\right)=1$. 因为 $\frac{\delta}{a}$、$\frac{\delta}{b}$ 是整数,当然 δ 是 a、b 的公倍数,所以 $\delta\vdots\delta'$. 設 $\delta=\delta' q$, 这里 $q>1$（如果 $q=1$, 那末 $\delta=\delta'$）. 这样

$$\left(\frac{\delta}{a},\ \frac{\delta}{b}\right)=\left(\frac{\delta' q}{a},\ \frac{\delta' q}{b}\right)=\left(\frac{\delta'}{a},\ \frac{\delta'}{b}\right)\cdot q=q>1.$$

上面的結果与条件 $\left(\frac{\delta}{a},\ \frac{\delta}{b}\right)=1$ 矛盾. 所以 $[a, b]=\delta$.

推論 如果 $(a, b)=1$, 那末 $[a, b]=ab$.

証明 因为 $ab \vdots a$，$ab \vdots b$，且 $\left(\frac{ab}{a}, \frac{ab}{b}\right)=(b, a)=1$，所以 $[a, b]=ab$.

4．如果 $[a, b]=\delta$，那末 $[ma, mb]=m\delta$.

証明 由 $[a, b]=\delta$，知 $\delta \vdots a$，$\delta \vdots b$. 所以 $m\delta \vdots ma$，$m\delta \vdots mb$. 由性質 3 得 $\left(\frac{\delta}{a}, \frac{\delta}{b}\right)=1$，所以 $\left(\frac{m\delta}{ma}, \frac{m\delta}{mb}\right)=\left(\frac{\delta}{a}, \frac{\delta}{b}\right)=1$. 这样，由性質 3 得 $[ma, mb]=m\delta$.

推論 1 如果 $[a, b]=\delta$，而 $a \vdots n$，$b \vdots n$，那末 $\left[\frac{a}{n}, \frac{b}{n}\right]=\frac{\delta}{n}$.

証明留給讀者.

推論 2 如果 $(a, c)=1$，那末 $[a, bc]=c[a, b]$.

証明 設 $[a, bc]=\delta$，显然 $\delta \vdots a$，$\delta \vdots c$. 因为 $(a, c)=1$，所以 $\delta \vdots ac$. 于是 $[ac, bc]=\delta$.

所以 $[a, bc]=[ac, bc]=c[a, b]$.

5．两数的最小公倍数是两数的乘积除以两数的最大公約数的商.

証明 設 $(a, b)=d$，于是 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

因为 $[a, b]=d\left[\frac{a}{d}, \frac{b}{d}\right]$，而 $\left[\frac{a}{d}, \frac{b}{d}\right]=\frac{ab}{d^2}$.

所以 $[a, b]=d\cdot\frac{ab}{d^2}=\frac{ab}{d}=\frac{ab}{(a, b)}$.

推論 $[a^s, b^s]=[a, b]^s$.

証明 因为 $[a^s, b^s]=\frac{a^s b^s}{(a^s, b^s)}$，而 $(a^s, b^s)=(a, b)^s$，所以

$$[a^s, b^s]=\frac{a^s b^s}{(a, b)^s}=[a, b]^s.$$

下面討論关于多个数的最小公倍数的性質.

6．設 $[a_1, a_2]=\delta_1$，$[\delta_1, a_3]=\delta_2$，$[\delta_2, a_4]=\delta_3$，……，$[\delta_{n-2}, a_n]=\delta_{n-1}$，那末 $[a_1, a_2, \cdots\cdots, a_n]=\delta_{n-1}$.

証明 根据所設条件，$\delta_{n-1} \vdots \delta_{n-2}$，$\delta_{n-2} \vdots \delta_{n-3}$，……，$\delta_3 \vdots \delta_2$，$\delta_2 \vdots \delta_1$，也就是 δ_{n-1} 是 δ_{n-1}，δ_{n-2}，δ_{n-3}，……，δ_3，δ_2，δ_1 这些数的公倍数．又因为 $\delta_{n-1} \vdots a_n$，$\delta_{n-2} \vdots a_{n-1}$，……，$\delta_2 \vdots a_3$，$\delta_1 \vdots a_2$，$\delta_1 \vdots a_1$，所以 δ_{n-1} 是 a_1，a_2，……，a_{n-1}，a_n 这些数的公倍数．

其次，如果 $[a_1, a_2, \cdots\cdots, a_n]=\delta_k<\delta_{n-1}$，于是 $\delta_k \vdots a_1$，$\delta_k \vdots a_2$，$\delta_k \vdots a_3$，……，$\delta_k \vdots a_n$．

已知 $[a_1, a_2]=\delta_1$，所以 $\delta_k \vdots \delta_1$；

已知 $[\delta_1, a_3]=\delta_2$，所以 $\delta_k \vdots \delta_2$；

…………………………………；

已知 $[\delta_{n-2}, a_n]=\delta_{n-1}$，所以 $\delta_k \vdots \delta_{n-1}$．

要使 $\delta_k \vdots \delta_{n-1}$，就必須存在 $\delta_k \geqslant \delta_{n-1}$，这就与假定的 $\delta_k<\delta_{n-1}$ 矛盾．所以 $[a_1, a_2, \cdots\cdots, a_n]=\delta_{n-1}$．

推論 1 如果 $[a_1, a_2, \cdots\cdots, a_k]=\delta$，那末

$$[a_1, a_2, \cdots\cdots, a_n]=[\delta, a_{k+1}, \cdots\cdots, a_n].$$

証明 設 $[a_1, a_2]=\delta_1$，$[\delta_1, a_3]=\delta_2$，……，$[\delta_{k-2}, a_k]=\delta_{k-1}$，……，$[\delta_{n-2}, a_n]=\delta_{n-1}$；也就是說，$[a_1, a_2, \cdots\cdots, a_n]=\delta_{n-1}$，又 $[a_1, a_2, \cdots\cdots, a_k]=\delta_{k-1}$ $(\delta_{k-1}=\delta)$．

由 $[\delta_{k-1}, a_{k+1}]=\delta_k$，$[\delta_k, a_{k+2}]=\delta_{k+1}$，……，$[\delta_{n-2}, a_n]=\delta_{n-1}$，可知 $[\delta_{k-1}, a_{k+1}, \cdots\cdots, a_n]=\delta_{n-1}$．就是 $[\delta, a_{k+1}, \cdots\cdots, a_n]=\delta_{n-1}$．

所以 $[a_1, a_2, \cdots\cdots, a_n]=[\delta, a_{k+1}, \cdots\cdots, a_n]$．

推論 2 如果 $[a_1, a_2, \cdots\cdots, a_k]=\delta$，$[a_{k+1}, \cdots\cdots, a_n]=\delta'$，那末

$$[a_1, a_2, \cdots\cdots, a_n]=[\delta, \delta'].$$

証明 因为 $[a_1, a_2, \cdots\cdots, a_n]=[\delta, a_{k+1}, \cdots\cdots, a_n]=[a_{k+1}, \cdots\cdots, a_n, \delta]$，又由推論 1 可知 $[a_{k+1}, \cdots\cdots, a_n, \delta]=[\delta', \delta]$．

所以 $[a_1, a_2, \cdots\cdots, a_n]=[\delta, \delta']$．

推論 3 如果 a_1，a_2，……，a_n 两两互質，那末

$$[a_1, a_2, \cdots\cdots, a_n]=a_1a_2\cdots\cdots a_n.$$

証明 設 $[a_1, a_2]=\delta_1$，$[\delta_1, a_3]=\delta_2$，……，$[\delta_{n-2}, a_n]=\delta_{n-1}$．

因为 $(a_1, a_2)=1$，所以 $\delta_1=a_1a_2$. 因为 $(a_1a_2, a_3)=1$，所以 $\delta_2=[\delta_1, a_3]=[a_1a_2, a_3]=a_1a_2a_3$. 同理，得 $\delta_4=[\delta_2, a_4]=[a_1a_2a_3, a_4]=a_1a_2a_3a_4$. 这样继續下去就得到：

$$[a_1, a_2, \cdots\cdots, a_n]=a_1a_2\cdots\cdots a_n.$$

推論 4 $[a_1^s, a_2^s, \cdots\cdots, a_n^s]=[a_1, a_2, \cdots\cdots, a_n]^s$.

証明 設 $[a_1, a_2]=\delta_1$, $[\delta_1, a_3]=\delta_2$, $\cdots\cdots$, $[\delta_{n-2}, a_n]=\delta_{n-1}$. 也就是 $[a_1, a_2, \cdots\cdots, a_n]=\delta_{n-1}$.

由性质 5 的推論，可以知道

$$[a_1^s, a_2^s]=\delta_1^s, [\delta_1^s, a_3^s]=\delta_2^s, \cdots\cdots, [\delta_{n-2}^s, a_n^s]=\delta_{n-1}^s.$$

所以 $[a_1^s, a_2^s, \cdots\cdots, a_n^s]=[a_1, a_2, \cdots\cdots, a_n]^s$.

7. 如果 $M, a_1, a_2, \cdots\cdots, a_n$ 是正整数，那末 $M \vdots [a_1, a_2, \cdots\cdots, a_n]$ 的充分而且必要条件是：

$$M \vdots a_1, \ M \vdots a_2, \ \cdots\cdots, \ M \vdots a_n.$$

証明 关于条件的充分性：

設 $[a_1, a_2]=\delta_1$, $[\delta_1, a_3]=\delta_2$, $\cdots\cdots$, $[\delta_{n-2}, a_n]=\delta_{n-1}$, 于是 $[a_1, a_2, \cdots\cdots, a_n]=\delta_{n-1}$.

已知 $[a_1, a_2]=\delta_1$，而 $M \vdots a_1$, $M \vdots a_2$，所以 $M \vdots \delta_1$;

已知 $[\delta_1, a_3]=\delta_2$，而 $M \vdots \delta_1$, $M \vdots a_3$，所以 $M \vdots \delta_2$;

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$;

已知 $[\delta_{n-2}, a_n]=\delta_{n-1}$，而 $M \vdots \delta_{n-2}$, $M \vdots a_n$，所以 $M \vdots \delta_{n-1}$.

这就証明了条件的充分性．关于条件的必要性的証明极簡单，这里从略．

8. 如果 $a_1, a_2, \cdots\cdots, a_n, \delta$ 是任意正整数，那末 $[a_1, a_2, \cdots\cdots, a_n]=\delta$ 的充分而且必要条件是：

$$\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=1.$$

証明 关于条件的必要性：

設 $\delta=a_1q_1=a_2q_2=\cdots\cdots=a_nq_n$，就是需要証明：

$$\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=(q_1, q_2, \cdots\cdots, q_n)=1.$$

如果 $(q_1, q_2, \cdots\cdots, q_n)=d>1$，又設 $q_1=dp_1, q_2=dp_2, \cdots\cdots, q_n=dp_n$，于是得 $\delta=a_1dp_1=a_2dp_2=\cdots\cdots=a_ndp_n$. 也就是，$\frac{\delta}{d}=a_1p_1=a_2p_2=\cdots\cdots=a_np_n$. 如果設 $\frac{\delta}{d}=\delta'$，由于 $d>1$，那末 $\delta'<\delta$. 而 δ' 是 $a_1, a_2, \cdots\cdots, a_n$ 等数的公倍数，这显然与条件 $[a_1, a_2, \cdots\cdots, a_n]=\delta$ 矛盾. 所以 $(q_1, q_2, \cdots\cdots, q_n)=1$.

关于条件的充分性：

設 $[a_1, a_2, \cdots\cdots, a_n]=\delta'\neq\delta$，那末 $\left(\frac{\delta'}{a_1}, \frac{\delta'}{a_2}, \cdots\cdots, \frac{\delta'}{a_n}\right)=1$. 因为 $\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}$ 都是整数，也就是說，δ 也是 $a_1, a_2, \cdots\cdots, a_n$ 的公倍数. 由性质 7 可以知道 $\delta \vdots \delta'$. 設 $\delta=\delta'q$，这里 $q>1$（$q=1$ 即意味着 $\delta=\delta'$），那末 $\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=\left(\frac{\delta'q}{a_1}, \frac{\delta'q}{a_2}, \cdots\cdots, \frac{\delta'q}{a_n}\right)=\left(\frac{\delta'}{a_1}, \frac{\delta'}{a_2}, \cdots\cdots, \frac{\delta'}{a_n}\right)\cdot q=q>1$. 这就与条件 $\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=1$ 矛盾. 所以 $[a_1, a_2, \cdots\cdots, a_n]=\delta$.

9. 設 $[a_1, a_2, \cdots\cdots, a_n]=\delta$，那末 $[ma_1, ma_2, \cdots\cdots, ma_n]=m\delta$.

証明 因为 $\delta \vdots a_1, \delta \vdots a_2, \cdots\cdots, \delta \vdots a_n$，所以 $m\delta \vdots ma_1, m\delta \vdots ma_2, \cdots\cdots, m\delta \vdots ma_n$. 又由条件可得：

$$\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=1.$$

这样 $\left(\frac{m\delta}{ma_1}, \frac{m\delta}{ma_2}, \cdots\cdots, \frac{m\delta}{ma_n}\right)=\left(\frac{\delta}{a_1}, \frac{\delta}{a_2}, \cdots\cdots, \frac{\delta}{a_n}\right)=1.$

所以 $[ma_1, ma_2, \cdots\cdots, ma_n]=m\delta.$

推論 如果 $[a_1, a_2, \cdots\cdots, a_n]=\delta$，而 $a_1, a_2, \cdots\cdots, a_n$ 都能被

k 整除，那末 $\left[\frac{a_1}{k}, \frac{a_2}{k}, \cdots\cdots, \frac{a_n}{k}\right]=\frac{\delta}{k}$.

証明留給讀者.

10. 如果 n 个数 $a_1, a_2, \cdots\cdots, a_k, a_{k+1}, \cdots\cdots, a_n$ 中，$a_1, a_2, \cdots\cdots, a_k$ 都能被 d 整除，而 $a_{k+1}, \cdots\cdots, a_n$ 都与 d 互質，那末

$$[a_1, a_2, \cdots\cdots, a_n]=d\left[\frac{a_1}{d}, \frac{a_2}{d}, \cdots\cdots, \frac{a_k}{d}, a_{k+1}, \cdots\cdots, a_n\right].$$

証明 設 $[a_1, a_2, \cdots\cdots, a_n]=\delta$, 又 $a_1=dq_1, a_2=dq_2, \cdots\cdots, a_k=dq_k$. 很明显，$\delta \vdots d$. 同时因为 $\delta \vdots a_{k+1}, \cdots\cdots, \delta \vdots a_n$，而 $a_{k+1}, \cdots\cdots, a_n$ 都与 d 互質，所以

$$\delta \vdots da_{k+1}, \cdots\cdots, \delta \vdots da_n.$$

于是 $[dq_1, dq_2, \cdots\cdots, dq_k, da_{k+1}, \cdots\cdots, da_n]=\delta$. 也就是 $\delta=d[q_1, q_2, \cdots\cdots, q_k, a_{k+1}, \cdots\cdots, a_n]$.

所以 $[a_1, a_2, \cdots\cdots, a_n]=d\left[\frac{a_1}{d}, \frac{a_2}{d}, \cdots\cdots, \frac{a_k}{d}, a_{k+1}, \cdots\cdots, a_n\right]$.

有了以上的一些性質，我們就有条件来探討如何求若干个数的最大公約数、最小公倍数的問題. 不过，如果要求圓滿地解决这个問題，还得具有数的分解的知識. 很明显，要解决数的分解問題，就应先掌握如何判断一数能否整除另一数的間題.

下面就分章討論有关数的整除性判别法以及数的分解方面的問題. 当然，这些内容的設置不仅是为了求若干数的最大公約数和最小公倍数；事实上，这两方面的内容是非常丰富的.

第二章 数的整除性判别法

一个数能不能被另一个数整除，例如，3360207 能不能被 167 整除，如果我們不用除法判别的話，有沒有其他方法呢？这一章的内容，就是用来解决这个問題的. 整除性判别法，就是：对于整数 N、D，为了

要判别"N能否被D整除",就找出另一个整数A($|A|<|N|$),使判别"N能否被D整除"簡化成只需判别"A能否被D整除".这个整数A,叫做判别数.

所謂一种好的整除性判别法,就是指判别数A的求法很簡捷的那种判别法.

在这一章里,我們将会看到三条定理(事实上,最后一条定理是前面两条的推广),这些定理是我們能比較完善地解决整除性的判别問題的理論根据.

为了書写方便,我們規定下面一些符号的意义:

1. 数 $N=10^n a_n+10^{n-1}a_{n-1}+\cdots\cdots+10a_1+a_0$,

a_i是非負整数,$0\leqslant a_i\leqslant 9$.

用下面記号表示:

$$N=\overline{a_n a_{n-1}\cdots\cdots a_1 a_0}.$$

2. 把N从右向左,每k位数字看做一节,如果共分为$t+1$节.我們把从右向左的每一节的数字所构成的数分别用下面的記号表示:

$$A_{0(k)},\ A_{1(k)},\ A_{2(k)},\ \cdots\cdots,\ A_{t(k)}.$$

譬如,对于$N=34675231$;

$$A_{0(2)}=31;\quad A_{1(2)}=52;\quad A_{2(2)}=67;\quad A_{3(2)}=34.$$

而 $A_{0(3)}=231$; $A_{1(3)}=675$; $A_{2(3)}=34$.

很明显,
$$\begin{aligned}N&=\overline{a_n a_{n-1}\cdots\cdots a_1 a_0}\\&=10^{tk}A_{t(k)}+10^{(t-1)k}A_{t-1(k)}+\cdots\cdots+10^k A_{1(k)}+A_{0(k)}.\end{aligned}$$

例如,
$$\begin{aligned}N&=34675231\\&=10^6 A_{3(2)}+10^4 A_{2(2)}+10^2 A_{1(2)}+A_{0(2)}\\&=10^6\cdot 34+10^4\cdot 67+10^2\cdot 52+31.\end{aligned}$$

$$\begin{aligned}N&=34675231\\&=10^6 A_{2(3)}+10^3 A_{1(3)}+A_{0(3)}\\&=10^6\cdot 34+10^3\cdot 675+231.\end{aligned}$$

3. 我們把"論断A成立的充分而且必要条件是論断B成立"用下

面的記号表示:

$$A \rightleftarrows B.$$

很明显,(1) 如果 $A \rightleftarrows B$, 那末 $B \rightleftarrows A$.

(2) 如果 $A \rightleftarrows B$, $B \rightleftarrows C$, 那末 $A \rightleftarrows C$.

4. 我們把"a 不被 b 整除"表示成:

$$a \text{不} \vdots\, b.$$

§1 D 是 $10^k - M$ 的約数

在研究一般情形之前,先研究几个特殊情形.

1. 当 $M=0$ 的时候:

如果$10^k \vdots D$, 那末 $N \vdots D \rightleftarrows A \vdots D$. ($A=\overline{a_{k-1}\cdots\cdots a_1 a_0}$)

証明 因为 $N - A = \overline{a_n\cdots\cdots a_1 a_0} - \overline{a_{k-1}\cdots\cdots a_1 a_0} = \overline{a_n\cdots\cdots a_k}\cdot 10^k$ $\vdots D$, 所以,如果 $A \vdots D$,一定可以推得 $N \vdots D$. 反过来,如果 $N \vdots D$, 也一定可以推得 $A \vdots D$. 这就証实了 $N \vdots D$ 的充要条件是 $A \vdots D$.

因此,当 $D=2^p\cdot 5^q$ (p, q 是非負整数) 的时候,就可以应用上述法则.

例 1 判别 6073128 能否被 8 整除.

因为 $10^3 \vdots 8$ ($8=2^3$), 所以只需判别 128 能否被 8 整除. 因为 $128 \vdots 8$, 所以 $6073128 \vdots 8$.

例 2 判别 28335 能否被 25 整除.

因为 $10^2 \vdots 25$, 所以只需判别 35 能否被 25 整除. 因为 35 不$\vdots$ 25, 所以 28335 不$\vdots$ 25.

例 3 判别 26368 能否被 250 整除.

因为 $10^3 \vdots 250$ ($250=2\cdot 5^3$), 所以只需判别 368 能否被 250 整除. 显然 368 不$\vdots$ 250, 所以 26368 不$\vdots$ 250.

当 $D=2^k$ 的时候, 虽然可以应用上面的法则, 然而应用下面的法则却更为簡便:

如果 $D=2^k$, 那末

$N:D \rightleftarrows A:D$. $(A=2^{k-1}a_{k-1}+2^{k-2}a_{k-2}+\overline{a_{k-3}\cdots\cdots a_1a_0})$

証明 已知 $N:D \rightleftarrows \overline{a_{k-1}\cdots\cdots a_1a_0}:D$, 所以只需証明:

$\overline{a_{k-1}\cdots\cdots a_1a_0}:D \rightleftarrows 2^{k-1}a_{k-1}+2^{k-2}a_{k-2}+\overline{a_{k-3}\cdots\cdots a_1a_0}:D$.

观察 $\overline{a_{k-1}\cdots\cdots a_1a_0}-(2^{k-1}a_{k-1}+2^{k-2}a_{k-2}+\overline{a_{k-3}\cdots\cdots a_1a_0})$

$=(10^{k-1}-2^{k-1})a_{k-1}+(10^{k-2}-2^{k-2})a_{k-2}$.

因为 $10^{k-2}-2^{k-2}=8(10^{k-3}+10^{k-4}\cdot 2+\cdots\cdots+10\cdot 2^{k-4}+2^{k-3})$, 这里 $8:2^3$, 而括号内的数能被 2^{k-3} 整除, 于是 $10^{k-2}-2^{k-2}:2^k$. 当然 $10^{k-1}-2^{k-1}:2^k$. 所以

$$\overline{a_{k-1}\cdots\cdots a_1a_0}-A:2^k\ (2^k=D).$$

于是容易推得 $\overline{a_{k-1}\cdots\cdots a_1a_0}:D \rightleftarrows A:D$.

特別地,当 $D=2^k$, 而 k 是奇数的时候,

$N:D \rightleftarrows 2^{k-1}a_{k-1}+2^{k-2}a_{k-2}+2^{k-3}a_{k-3}+\overline{a_{k-4}\cdots\cdots a_1a_0}:D$.

关于这一点留給讀者証明.

例 1 試想出一种判别法,可用来判别 N 能否被 8 整除.

因为 $8=2^3$, 而 3 是奇数, 所以得到下面的判别法:

$$N:8 \rightleftarrows 2^2a_2+2a_1+a_0:8.$$

例 2 判别 52732 能否被 16 整除.

因为 $16=2^4$, 而 $A=2^3\cdot 2+2^2\cdot 7+32=76$, 所以只需判别 76 能否被 16 整除. 因为 76 不 $:16$, 所以 52732 不 $:16$.

例 3 判别 436000 能否被 32 整除.

因为 $32=2^5$, 而 $A=2^4\cdot 3+2^3\cdot 6=96:32$, 所以 $436000:32$.

2. 当 $M=1$ 的时候:

如果 $10^k-1:D$, 那末

(1) $N:D \rightleftarrows A:D$; $[A=A_{0(k)}+A_{1(k)}+\cdots\cdots+A_{t(k)}]$

(2) $N:D \rightleftarrows A':D$. $[A'=\overline{a_n\cdots\cdots a_{k+1}a_k}+A_{0(k)}]$

証明 (1)

因为 $N-A=(10^{tk}A_{t(k)}+10^{(t-1)k}A_{t-1(k)}+\cdots\cdots+10^kA_{1(k)}+A_{0(k)})$

$-(A_{t(k)}+A_{t-1(k)}+\cdots\cdots+A_{1(k)}+A_{0(k)})$

$$=(10^{tk}-1)A_{t(k)}+(10^{(t-1)k}-1)A_{t-1(k)}+\cdots\cdots$$
$$+(10^k-1)A_{1(k)}.$$

显然，等式右边的每一項都能被 10^k-1 整除，也就是 $N-A \vdots 10^k-1$. 因此 $N-A \vdots D$. 所以 $N \vdots D \rightleftarrows A \vdots D$.

关于(2)的証明留給讀者.

例 1 判别 324675 能否被 9 整除.

因为 $10^1-1 \vdots 9$，而 $A=5+7+6+4+2+3=27$，所以只需判别 27 能否被 9 整除. 因为 $27 \vdots 9$，所以 $324675 \vdots 9$.

例 2 判别 74234501 能否被 11 整除.

因为 $10^2-1 \vdots 11$，而 $A=1+45+23+74=143$，由第一个方法知道只需判别 143 能否被 11 整除；这就需要判别 43+1 能否被 11 整除. 因为 $44 \vdots 11$，于是 $143 \vdots 11$，所以可以推得 $74234501 \vdots 11$.

这也可以根据第二个方法来判别：

首先因为 $A'=742345+1=742346$，就要判别 742346 能否被 11 整除. 这里因为 7423+46=7469，就需判别 7469 能否被 11 整除. 又因为 74+69=143，于是就需判别 143 能否被 11 整除. 显然，$1+43=44 \vdots 11$. 这样，向上推去，就可以得到 $74234501 \vdots 11$.

为了叙述方便，可把判别过程中所用的运算安排如下：

```
       7 4 2 3 4 5(0 1)
    +)           0 1
    ----------------
       7 4 2 3(4 6)
    +)       4 6
    -------------
       7 4(6 9)
   +) 6 9
   ---------
     1(4 3)          ∵      44 ⋮ 11,
+) 4 3               ∴ 74234501 ⋮ 11.
-----------
   4 4
```

例 3 判别 62123 能否被 37 整除.

因为 $10^3-1(3^3\cdot 37)\vdots 37$，而 $123+62=185$，所以只需判别 185 能否被 37 整除，因为 $185\vdots 37$，所以 $62123\vdots 37$.

这个法则，如果取 $k=1$，就适用于 $10^1-1\vdots D$（即 D 是 3、9）的时候；如果取 $k=2$，就适用于 $10^2-1\vdots D$（例如 D 是 11、33、99）的时候；如果取 $k=3$，就适用于 $10^3-1\vdots D$（例如 D 是 27、37、111、333、999）的时候；如果取 $k=4$，就适用于 $10^4-1\vdots D$（例如，D 是 101、303、909、1111、3333、9999）的时候；等等.

3．当 $M=-1$ 的时候：

如果 $10^k+1\vdots D$，那末

(1) $N\vdots D \rightleftarrows A\vdots D$；$(A=A_{0(k)}-A_{1(k)}+\cdots\cdots+(-1)^t A_{t(k)}$

$$=[A_{0(k)}+A_{2(k)}+\cdots\cdots]-[A_{1(k)}+A_{3(k)}+\cdots\cdots])$$

(2) $N\vdots D \rightleftarrows A'\vdots D$.$(A'=\overline{a_n\cdots\cdots a_{k+1}a_k}-A_{0(k)})$

証明(1)

$$\begin{aligned} N-A&=[A_{0(k)}+10^k A_{1(k)}+\cdots\cdots+10^{tk}A_{t(k)}]\\ &\quad-[A_{0(k)}-A_{1(k)}+\cdots\cdots+(-1)^t A_{t(k)}]\\ &=(10^k+1)A_{1(k)}+(10^{2k}-1)A_{2(k)}+\cdots\cdots\\ &\quad+[10^{tk}-(-1)^t]A_{t(k)}. \end{aligned}$$

而

$$10^k+1\vdots 10^k+1,$$
$$10^{2k}-1\vdots 10^k+1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

当 t 是偶数的时候，$10^{tk}-(-1)^t=10^{tk}-1\vdots 10^k+1$，

当 t 是奇数的时候，$10^{tk}-(-1)^t=10^{tk}+1\vdots 10^k+1$.

于是 $N-A\vdots 10^k+1$，也就是 $N-A\vdots D$. 从而可推出

$$N\vdots D \rightleftarrows A\vdots D.$$

关于(2)的証明留給讀者.

例 1 判别 345750209 能否被 7 整除.

因为 $10^3+1(10^3+1=7\cdot 11\cdot 13)\vdots 7$，可以用第一个方法判别：这里 $A=209-750+345=(209+345)-750=-196$，所以只需判

别-196能否被7整除.因为$196 \vdots 7$,也就是$-196 \vdots 7$,所以$345750209 \vdots 7$.

这也可以用第二个方法判别：我們把判别所用的計算安排如下：

$$
\begin{array}{rl}
 & 3\ 4\ 5\ 7\ 5\ 0(2\ 0\ 9) \\
-) & \qquad\ \ 2\ 0\ 9 \\
\hline
 & 3\ 4\ 5(5\ 4\ 1) \\
-) & 5\ 4\ 1 \\
\hline
 & -1\ 9\ 6
\end{array}
$$

因为$196 \vdots 7$，所以$345750209 \vdots 7$.

例2 判别74234501能否被11整除.

因为$10^3+1 \vdots 11$,所以这个例题可和上例一样解决.但是$10+1 \vdots 11$,所以我們就可以这样来判别：因为$A=(1+5+3+4)-(0+4+2+7)=0$，显然，$0 \vdots 11$，所以$74234501 \vdots 11$.

例3 判别981720能否被101整除.

因为$10^2+1 \vdots 101$，可用第一个方法来判别.

因为$A=(20+98)-17=101 \vdots 101$，所以$981720 \vdots 101$.

用第二个方法来判别：

$$
\begin{array}{rl}
 & 9\ 8\ 1\ 7(2\ 0) \\
-) & \qquad 2\ 0 \\
\hline
 & 9\ 7(9\ 7) \\
-) & 9\ 7 \\
\hline
 & \quad 0
\end{array}
$$

因为$0 \vdots 101$，所以$981720 \vdots 101$.

这条法則,如果取$k=1$，就适用于$10^1+1 \vdots D$（即D等于11）的时候;如果取$k=2$，就适用于$10^2+1 \vdots D$（即D等于101）的时候；如果取$k=3$，就适用于$10^3+1 \vdots D$（即D等于7、11、13、77、91、143、1001)的时候;如果取$k=4$，就适用于$10^4+1 \vdots D$（即D等于73、137、10001)的时候;等等.

4．当 $M=2$ 的时候：

如果 $10^k-2 \vdots D$，那末

(1) $N \vdots D \rightleftarrows A \vdots D$;

$$[A=A_{0(k)}+2A_{1(k)}+2^2A_{2(k)}+\cdots\cdots+2^tA_{t(k)}]$$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}\cdot 2+A_{0(k)}]$

当 $M=-2$ 的时候：

如果 $10^k+2 \vdots D$，那末

(1) $N \vdots D \rightleftarrows A \vdots D$;

$$[A=A_{0(k)}-2A_{1(k)}+2^2A_{2(k)}-\cdots\cdots+(-2)^tA_{t(k)}]$$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}\cdot(-2)+A_{0(k)}]$

法则的証明留給讀者.

例1 判别 14994950 能否被 499 整除.

因为 $10^3-2 \vdots 499$，所以

(1) $N \vdots 499 \rightleftarrows A_{0(3)}+2A_{1(3)}+\cdots\cdots+2^tA_{t(3)} \vdots 499$;

(2) $N \vdots 499 \rightleftarrows \overline{a_n\cdots\cdots a_3}\cdot 2+\overline{a_2a_1a_0} \vdots 499$.

由(1)来判别：这里只需判别 A 能否被 499 整除.因为 $A=950+2\cdot 994+2^2\cdot 14=(14\cdot 2+994)\cdot 2+950$，所以数 A 的求法可安排如下：

$$\begin{array}{rl} 14 & (\cdot 2) \\ +)\ 994 & \\ \hline 1022 & (\cdot 2) \\ +)\ 950 & \\ \hline 2994 & =A \end{array}$$

至于 2994 能否被 499 整除，可以用上面方法同样处理：因为 $994+2\cdot 2=998 \vdots 499$，也就是 $2994 \vdots 499$.

所以 $14994950 \vdots 499$.

由(2)来判别：这里 $A'=14994\cdot 2+950=30938$，所以只需判别 30938 能否被 499 整除.因为 $30\cdot 2+938=998$，于是,就需判别 998 能否被 499 整除. 因为 $998 \vdots 499$，也就是 $30938 \vdots 499$，所以 14994950

$\vdots$ 499.

例 2 試判别 3360207 能否被 167 整除.

因为 $10^3+2 \vdots 167$, 所以

(1) $N \vdots 167 \rightleftarrows A_{0(3)}-2A_{1(3)}+\cdots\cdots+(-2)^t A_{t(3)} \vdots 167$;

(2) $N \vdots 167 \rightleftarrows \overline{a_n \cdots\cdots a_3}\cdot(-2)+A_{0(3)} \vdots 167$.

由(1)来判别：这里只需判别 A 能否被167整除，而 $A=207-2\cdot360+(-2)^2\cdot3=[3\cdot(-2)+360]\cdot(-2)+207$，所以数 A 的求法可安排如下：

$$
\begin{array}{rl}
3 & [\cdot(-2)] \\
+)\ 3\ 6\ 0 & \\
\hline
3\ 5\ 4 & [\cdot(-2)] \\
+)\ 2\ 0\ 7 & \\
\hline
-\ 5\ 0\ 1 & = A
\end{array}
$$

$\because$ 501 $\vdots$ 167 (即 $-501 \vdots 167$)， $\therefore$ 3360207 $\vdots$ 167.

由(2)来判别：因为 $A'=3360\cdot(-2)+207=-6513$，首先判别 -6513，能否被 167 整除. 由于 $6\cdot(-2)+513=501$，从而只需判别 501 能否被 167 整除. 因为 501 $\vdots$ 167，所以可推得 3360207 $\vdots$ 167.

关于 $M=2$ 的那条法則，如果取 $k=1$，就适用于 $10-2 \vdots D$（即 D 等于 2、4、8）的时候；如果 $k=2$，就适用于 $10^2-2 \vdots D$（譬如 D 等于 7、14、49）的时候；如果取 $k=3$，就适用于 $10^3-2 \vdots D$（譬如 D 等于 499、998）的时候；等等.

关于 $M=-2$ 的那条法則，如果取 $k=1$，就适用于 $10+2 \vdots D$（例如 D 等于 6、12）的时候；如果取 $k=2$，就适用于 $10^2+2 \vdots D$（例如 D 等于 17、34、51、102）的时候；如果取 $k=3$，就适用于 $10^3+2 \vdots D$（例如 D 等于 167、334、501、1002）的时候；等等.

5、上面研究了 M 等于 0、±1、±2 的几种特殊情形，即使是这几种情形，我們已經看到由它們可以創立不少有趣的整除性的判别法則. 現在来研究一条較为一般的定理.

定理 如果 $10^k-M \vdots D$（k 是正整数，M 是任意整数），那末

(1) $N \vdots D \rightleftarrows A \vdots D$; $[A=A_{0(k)}+MA_{1(k)}+\cdots\cdots+M^tA_{t(k)}]$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}\cdot M+A_{0(k)}]$

証明(1) $N-A$

$$=[10^{tk}A_{t(k)}+10^{(t-1)k}A_{t-1(k)}+\cdots\cdots+10^kA_{1(k)}+A_{0(k)}]$$
$$-[M^tA_{t(k)}+M^{t-1}A_{t-1(k)}+\cdots\cdots+MA_{1(k)}+A_{0(k)}]$$
$$=(10^{tk}-M^t)A_{t(k)}+(10^{(t-1)k}-M^{t-1})A_{t-1(k)}+\cdots\cdots$$
$$+(10^k-M)A_{1(k)}.$$

因为等式右边的每项都能被 10^k-M 整除，所以 $N-A \vdots 10^k-M$. 因此 $N-A \vdots D$. 这就推得了(1).

(2) $N-A'=[\overline{a_n\cdots\cdots a_k}\cdot 10^k+A_{0(k)}]-[\overline{a_n\cdots\cdots a_k}\cdot M+A_{0(k)}]$
$$=\overline{a_n\cdots\cdots a_k}(10^k-M).$$

显然，$N-A' \vdots 10^k-M$，也就是説，$N-A' \vdots D$。所以也推得了(2).

在具体应用定理之前，必須先安排一下求数 A 的运算方法，以便能簡捷地求出判别数.

数 $A=A_{0(k)}+MA_{1(k)}+\cdots\cdots+M^tA_{t(k)}$，可用下法求得：

$$\begin{array}{rl}
A_{t(k)} & (\cdot M)\\
+)\quad A_{t-1(k)} & \\ \hline
A_{t-1(k)}+MA_{t(k)} & (\cdot M)\\
+)\quad A_{t-2(k)} & \\ \hline
\cdots\cdots\cdots\cdots & \\
+)\quad \cdots\cdots & \\ \hline
A_{1(k)}+MA_{2(k)}+\cdots\cdots+M^{t-1}A_{t(k)} & (\cdot M)\\
+)\quad A_{0(k)} & \\ \hline
A_{0(k)}+MA_{1(k)}+\cdots\cdots+M^tA_{t(k)} & =A
\end{array}$$

至于数 $A'=\overline{a_n\cdots\cdots a_k}\cdot M+A_{0(k)}$ 的求法比較簡单，这里可以从略.

例 1 判别 292067 能否被 97 整除。

因为 $10^2-3 \vdots 97$，就是 $k=2$、$M=3$. 所以

(1) $N \vdots 97 \rightleftarrows A_{0(2)}+3A_{1(2)}+\cdots\cdots+3^tA_{t(2)} \vdots 97$;

(2) $N \vdots 97 \rightleftarrows \overline{a_n\cdots\cdots a_2}\cdot 3+\overline{a_1a_0} \vdots 97$.

由(1)来判别：因为 $A=67+3\cdot 20+3^2\cdot 29=(29\cdot 3+20)\cdot 3+67$，它的計算可以安排如下：

$$\begin{array}{rl} 29 & (\cdot 3)\\ +)\ 20 & \\ \hline 107 & (\cdot 3)\\ +)\ 67 & \\ \hline 388 & =A \end{array}$$

当然，要判别 388 能否被 97 整除，可以用同样方法处理：因为 $88+3\cdot 3=97 \vdots 97$，就是 $388 \vdots 97$，所以 $292067 \vdots 97$.

由(2)来判别：

$$\begin{array}{rl} 2920 & (\cdot 3)\\ +)\ 67 & \\ \hline 8827 & \end{array}$$

判别 8827 能否被 97 整除，可以用同样方法处理：

$$\begin{array}{rl} 88 & (\cdot 3)\\ +)\ 27 & \\ \hline 291 & \end{array}$$

于是，就只需判别 291 能否被 97 整除．因为 $2\cdot 3+91=97 \vdots 97$，就是 $291 \vdots 97$，从而 $8827 \vdots 97$，所以得 $292067 \vdots 97$.

例 2 判别 2374723 能否被 13 整除．

因为 $10^3+1 \vdots 13$，又 $10+3 \vdots 13$，由上可得到两种判别法：

(1) $N \vdots 13 \rightleftarrows A_{0(3)}-A_{1(3)}+\cdots\cdots+(-1)^tA_{t(3)} \vdots 13$

(或 $N \vdots 13 \rightleftarrows \overline{a_n\cdots\cdots a_3}-\overline{a_2a_1a_0} \vdots 13$)；

(2) $N \vdots 13 \rightleftarrows a_0-3a_1+3^2a_2-\cdots\cdots+(-3)^na_n \vdots 13$

(或 $N \vdots 13 \rightleftarrows \overline{a_n\cdots\cdots a_2a_1}\cdot 3-a_0 \vdots 13$)．

我們可以把这两种方法結合起来应用．

先由(1)：因为 $723-374+2=351$，所以只需判别 351 能否被 13 整除．这就可以由(2)来完成：

因为$1-3\cdot5+3^2\cdot3=13\vdots13$，就是$351\vdots13$，所以推得$2374723\vdots13$.

例3 判别4039979能否被1999整除.

可以看到1999的5倍等于9995. 就是说，$10^4-5\vdots1999$. 这里得到$k=4$、$M=5$. 这就找到了判别法. 因为$9979+5\cdot403=11994$，于是就只需判别11994能否被1999整除. 因为$1994+5\cdot1=1999\vdots1999$，就知道$11994\vdots1999$，从而推得$4039979\vdots1999$.

例4 判别51860307能否被503整除.

显然，$10^3+6\vdots503$，就是$k=3$，$M=-6$. 这就表示找到了判别法.

$$\begin{array}{r l}
51 & [\cdot(-6)] \\
+)\ 860 & \\
\hline
554 & [\cdot(-6)] \\
+)\ 307 & \\
\hline
-3017 &
\end{array}$$

这就需要判别3017能否被503整除.

因为$17+(-6)\cdot3=-1$，而-1不$\vdots503$，就知道3017不$\vdots503$，所以51860307不$\vdots503$.

§2 D是$M\cdot10^k-1$的約数

在研究一般情形之前，先研究几个特殊情形.

至于$M=\pm1$的情形，显然，在上一节里已获得解决.

1. 当$M=2$的时候：

如果$2\cdot10^k-1\vdots D$，那末

(1) $N\vdots D\rightleftarrows A\vdots D$; $[A=A_{t(k)}+2A_{t-1(k)}+\cdots\cdots+2^tA_{0(k)}]$

(2) $N\vdots D\rightleftarrows A'\vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}+2A_{0(k)}]$

証明(1) 因为$2\cdot10^k-1\vdots D$，可以断言$(D,2)=1$，从而$(D,2^t)=1$. 这样，由$N\vdots D$可以推知$2^tN\vdots D$；反过来，也可以由$2^tN\vdots D$推知$N\vdots D$. 或 $N\vdots D\rightleftarrows2^tN\vdots D$.

于是問題就变成只需証明:

$$2^tN \vdots D \rightleftarrows A \vdots D.$$

$$\begin{aligned}&2^tN-A\\&=[2^t10^{tk}A_{t(k)}+2^t10^{(t-1)k}A_{t-1(k)}+\cdots\cdots+2^t10^kA_{1(k)}+2^tA_{0(k)}]\\&\quad-[A_{t(k)}+2A_{t-1(k)}+\cdots\cdots+2^{t-1}A_{1(k)}+2^tA_{0(k)}]\\&=[(2\cdot10^k)^t-1]A_{t(k)}+2[(2\cdot10^k)^{t-1}-1]A_{t-1(k)}+\cdots\cdots\\&\quad+2^{t-1}[2\cdot10^k-1]A_{1(k)}.\end{aligned}$$

显然,等式右边每項都能被 $2\cdot10^k-1$ 整除,也就是都能被 D 整除,因此 $2^tN-A \vdots D$. 于是可推得:

$$2^tN \vdots D \rightleftarrows A \vdots D.$$

关于(2)的証明留給讀者.

例1 判别 4029976 能否被 19 整除.

因为 $2\cdot10-1 \vdots 19$,所以

(1) $N \vdots 19 \rightleftarrows a_n+2\cdot a_{n-1}+\cdots\cdots+2^na_0 \vdots 19$;

(2) $N \vdots 19 \rightleftarrows \overline{a_n\cdots\cdots a_1}+2a_0 \vdots 19$.

由(1)来判别: $A=4+2\cdot0+2^2\cdot2+2^3\cdot9+2^4\cdot9+2^5\cdot7+2^6\cdot6$,我們把求 A 的运算安排如下:

$$\begin{array}{rl} 6 & (\cdot2)\\ +)\quad 7 & \\ \hline 19 & (\cdot2)\\ +)\quad 9 & \\ \hline 47 & (\cdot2)\\ +)\quad 9 & \\ \hline 103 & (\cdot2)\\ +)\quad 2 & \\ \hline 208 & (\cdot2)\\ +)\quad 0 & \\ \hline 416 & (\cdot2)\\ +)\quad 4 & \\ \hline 836 & =A \end{array}$$

于是只需判别 836 能否被 19 整除．这可以用同样方法处理：因为 $8+2\cdot3+2^2\cdot6=38\vdots19$，也就是 $836\vdots19$，从而 $4029976\vdots19$．

由(2)来判别：因为 $A'=402997+2\cdot6$，而 A' 的值仍很大，所以要判别 A' 能否被 19 整除，可以用同样方法处理．这样，我們可以把判别过程中所需的計算安排如下：

$$
\begin{array}{lr l}
 & 4\;0\;2\;9\;9\;7(6) & \\
+) & 1\;2 & (=2\cdot6) \\
\hline
 & 4\;0\;3\;0\;0(9) & \\
+) & 1\;8 & (=2\cdot9) \\
\hline
 & 4\;0\;3\;1(8) & \\
+) & 1\;6 & (=2\cdot8) \\
\hline
 & 4\;0\;4(7) & \\
+) & 1\;4 & (=2\cdot7) \\
\hline
 & 4\;1(8) & \\
+) & 1\;6 & (=2\cdot8) \\
\hline
 & 5\;7 &
\end{array}
$$

因为 $57\vdots19$，所以 $4029976\vdots19$．

例 2　判别 40021979 能否被 1999 整除．

上节中已采用过这个例子，这里当然要用另外的方法来解决它．

因为 $2\cdot10^3-1\vdots1999$，所以

(1)　$N\vdots1999 \rightleftarrows A_{t(3)}+2A_{t-1(3)}+\cdots\cdots+2^tA_{0(3)}\vdots1999$；

(2)　$N\vdots1999 \rightleftarrows \overline{a_n\cdots\cdots a_3}+2\cdot A_{0(3)}\vdots1999$．

由(1)来判别：$A=40+2\cdot21+2^2\cdot979$．所以可以把求 A 的运算安排如下：

$$
\begin{array}{lr l}
 & 9\;7\;9 & (\cdot2) \\
+) & 2\;1 & \\
\hline
 & 1\;9\;7\;9 & (\cdot2) \\
+) & 4\;0 & \\
\hline
 & 3\;9\;9\;8 & =A
\end{array}
$$

显然，$3998 \vdots 1999$，所以 $40021979 \vdots 1999$.

由(2)来判别：因为由(2)来判别，往往需要把法则連續地应用几次，所以把整个判别过程中的計算安排如下：

$$
\begin{array}{rl}
4\ 0\ 0\ 2\ 1(9\ 7\ 9) & \\
+)\quad 1\ 9\ 5\ 8 & (=2\cdot 979) \\
\hline
4\ 1(9\ 7\ 9) & \\
+)\ 1\ 9\ 5\ 8 & (=2\cdot 979) \\
\hline
1\ 9\ 9\ 9 &
\end{array}
$$

由結果可以知道：$40021979 \vdots 1999$.

2．当 $M=-2$ 的时候：

如果 $2\cdot 10^k+1 \vdots D$，那末

(1) $N \vdots D \rightleftarrows A \vdots D$;$[A=A_{t(k)}-2A_{t-1(k)}+\cdots\cdots+(-2)^t A_{0(k)}]$

(2) $N \vdots D \rightleftarrows A' \vdots D$.$[A'=\overline{a_n\cdots\cdots a_k}-2A_{0(k)}]$

証明部分留給讀者.

例 1 判别 148874 能否被 67 整除.

因为 $2\cdot 10^2+1 \vdots 67$，所以

(1) $N \vdots 67 \rightleftarrows A_{t(2)}-2A_{t-1(2)}+\cdots\cdots+(-2)^t A_{0(2)} \vdots 67$;

(2) $N \vdots 67 \rightleftarrows \overline{a_n\cdots\cdots a_2}-2\cdot\overline{a_1 a_0} \vdots 67$.

由(1)来判别：$A=14+88(-2)+74(-2)^2$. 所以可以把求 A 的运算安排如下：

$$
\begin{array}{rl}
7\ 4 & [\cdot(-2)] \\
+)\ 8\ 8 & \\
\hline
-6\ 0 & [\cdot(-2)] \\
+)\ 1\ 4 & \\
\hline
1\ 3\ 4 &
\end{array}
$$

因为 $134 \vdots 67$，所以 $148874 \vdots 67$.

由(2)来判别：判别过程中的全部計算安排如下：

$$
\begin{array}{rl}
 & 1\ 4\ 8\ 8(7\ 4) \\
-) & \quad 1\ 4\ 8 \qquad (=2\cdot 74) \\
\hline
 & 1\ 3(4\ 0) \\
-) & 8\ 0 \qquad\qquad (=2\cdot 40) \\
\hline
 & -6\ 7
\end{array}
$$

由結果可以推知：$148874 \vdots 67$.

例 2 判別 273347 能否被 6667 整除.

因为 $2\cdot 10^4+1 \vdots 6667$，这就說明找到了判別法．因为 $A=27+3347(-2)=-6667 \vdots 6667$，所以 $273347 \vdots 6667$.

3．現在来研究較为一般的情形．

定理 如果 $M\cdot 10^k-1 \vdots D$ (k 是正整数，M 是非零整数)，那末

(1) $N \vdots D \rightleftarrows A \vdots D$；$[A=A_{t(k)}+MA_{t-1(k)}+\cdots\cdots+M^t A_{0(k)}]$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}+MA_{0(k)}]$

証明(1) 由 $M\cdot 10^k-1 \vdots D$，可以断言 $(|M|, D)=1$，从而 $(|M^t|, D)=1$. 就有 $N \vdots D \rightleftarrows M^t N \vdots D$.

于是只需証明：$M^t N \vdots D \rightleftarrows A \vdots D$.

$$
\begin{aligned}
& M^t N-A \\
&=[M^t 10^{tk} A_{t(k)}+M^t 10^{(t-1)k} A_{t-1(k)}+\cdots\cdots+M^t 10^k A_{1(k)}+M^t A_{0(k)}] \\
&\quad -[A_{t(k)}+MA_{t-1(k)}+\cdots\cdots+M^{t-1} A_{1(k)}+M^t A_{0(k)}] \\
&=[(M10^k)^t-1]A_{t(k)}+M[(M10^k)^{t-1}-1]A_{t-1(k)}+\cdots\cdots \\
&\quad +M^{t-1}[M10^k-1]A_{1(k)}.
\end{aligned}
$$

显然，等式右边的每項都能被 $M10^k-1$ 整除，也就是都能被 D 整除，所以 $M^t N-A \vdots D$. 从而可以推得：

$$M^t N \vdots D \rightleftarrows A \vdots D.$$

(2) 因为 $N \vdots D \rightleftarrows MN \vdots D$，所以只需証明：

$$MN \vdots D \rightleftarrows A' \vdots D.$$

$$
\begin{aligned}
MN-A' &= [\overline{a_n\cdots\cdots a_k}\cdot M10^k+MA_{0(k)}]-[\overline{a_n\cdots\cdots a_k}+MA_{0(k)}] \\
&= \overline{a_n\cdots\cdots a_k}(M10^k-1) \vdots D.
\end{aligned}
$$

所以可以推得：$MN \vdots D \rightleftarrows A' \vdots D$。于是 $N \vdots D \rightleftarrows A' \vdots D$.

在具体地应用定理之前，先安排一下求数 A 的运算，以便簡捷地求出判別数.

数 $A = A_{t(k)} + MA_{t-1(k)} + \cdots\cdots + M^t A_{0(k)}$ 可由下法求出：

$$
\begin{array}{lr l}
 & A_{0(k)} & (\cdot M) \\
+) & A_{1(k)} & \\
\hline
 & A_{1(k)} + MA_{0(k)} & (\cdot M) \\
+) & A_{2(k)} & \\
\hline
 & \cdots\cdots\cdots\cdots & \\
+) & A_{t(k)} & \\
\hline
\end{array}
$$

$A_{t(k)} + MA_{t-1(k)} + \cdots\cdots + M^t A_{0(k)} = A$

至于数 $A' = \overline{a_n \cdots\cdots a_k} + MA_{0(k)}$，比較容易計算，这里从略.

例 1 判別 2674763 能否被 133 整除.

因为 $4 \cdot 10^2 - 1 \vdots 133$，这里 $k=2$，$M=4$. 所以

(1) $N \vdots 133 \rightleftarrows A_{t(2)} + 4A_{t-1(2)} + \cdots\cdots + 4^t A_{0(2)} \vdots 133$;

(2) $N \vdots 133 \rightleftarrows \overline{a_n \cdots\cdots a_2} + 4\overline{a_1 a_0} \vdots 133$.

由(1)来判别：

$$
\begin{array}{lr l}
 & 63 & (\cdot 4) \\
+) & 47 & \\
\hline
 & 299 & (\cdot 4) \\
+) & 67 & \\
\hline
 & 1263 & (\cdot 4) \\
+) & 2 & \\
\hline
 & 5054 & = A
\end{array}
$$

于是只需判别 5054 能否被 133 整除. 这可以用同样方法处理：

$$
\begin{array}{lr l}
 & 54 & (\cdot 4) \\
+) & 50 & \\
\hline
 & 266 &
\end{array}
$$

因为 266 ⋮ 133，就是 5054 ⋮ 133．从而 2674763 ⋮ 133．

由(2)来判别：

$$
\begin{array}{rrl}
 & 2\ 6\ 7\ 4\ 7(6\ 3) & \\
+) & 2\ 5\ 2 & (=4\cdot 63) \\
\hline
 & 2\ 6\ 9(9\ 9) & \\
+) & 3\ 9\ 6 & (=4\cdot 99) \\
\hline
 & 6\ 6\ 5 &
\end{array}
$$

因为 665 ⋮ 133，所以 2674763 ⋮ 133．

例 2　判别 14994950 能否被 499 整除．

上节中采用过这个例子，这里当然准备用本节中的定理来解．

因为 $5\cdot 10^2-1$ ⋮ 499，就是 $k=2$、$M=5$．这就找到了判别法：

(1)　$N \vdots 499 \rightleftarrows A_{t(2)}+5A_{t-1(2)}+\cdots\cdots+5^t A_{0(2)} \vdots 499$；

(2)　$N \vdots 499 \rightleftarrows \overline{a_n\cdots\cdots a_2}+5\overline{a_1a_0} \vdots 499$.

由(1)来判别：

$$
\begin{array}{rrl}
 & 5\ 0 & (\cdot 5) \\
+) & 4\ 9 & \\
\hline
 & 2\ 9\ 9 & (\cdot 5) \\
+) & 9\ 9 & \\
\hline
 & 1\ 5\ 9\ 4 & (\cdot 5) \\
+) & 1\ 4 & \\
\hline
 & 7\ 9\ 8\ 4 &
\end{array}
$$

于是只需判别 7984 能否被 499 整除．这可以用同样方法处理：

$$
\begin{array}{rrl}
 & 8\ 4 & (\cdot 5) \\
+) & 7\ 9 & \\
\hline
 & 4\ 9\ 9 &
\end{array}
$$

由結果可以知道 7984 ⋮ 499，所以 14994950 ⋮ 499．

由(2)来判别：

$$\begin{array}{r l}
& 1\ 4\ 9\ 9\ 4\ 9(5\ 0) \\
+) & 2\ 5\ 0 \quad (=5\cdot 50) \\
\hline
& 1\ 5\ 0\ 1(9\ 9) \\
+) & 4\ 9\ 5 \quad (=5\cdot 99) \\
\hline
& 1\ 9(9\ 6) \\
+) & 4\ 8\ 0 \quad (=5\cdot 96) \\
\hline
& 4\ 9\ 9
\end{array}$$

由結果可以推知 $14994950 \vdots 499$.

例 3 判别 912073 能否被 43 整除.

(1) 因为 $13\cdot 10-1 \vdots 43$, 就是 $k=1$, $M=13$. 这就找到了判别法. 我們挑第二个方法来判别:

$$\begin{array}{r l}
& 9\ 1\ 2\ 0\ 7(3) \\
+) & 3\ 9 \quad (=13\cdot 3) \\
\hline
& 9\ 1\ 2\ 4(6) \\
+) & 7\ 8 \quad (=13\cdot 6) \\
\hline
& 9\ 2\ 0(2) \\
+) & 2\ 6 \quad (=13\cdot 2) \\
\hline
& 9\ 4(6) \\
+) & 7\ 8 \quad (=13\cdot 6) \\
\hline
& 1\ 7(2) \\
+) & 2\ 6 \quad (=13\cdot 2) \\
\hline
& 4\ 3
\end{array}$$

因为 $43 \vdots 43$, 所以 $912073 \vdots 43$.

(2) 因为 $3\cdot 10^2+1(=301) \vdots 43$, 就是 $k=2$, $M=-3$. 这就找到了另外的一个判别法, 我們也挑其中的第二个方法来判别:

$$\begin{array}{r l}
& 9\ 1\ 2\ 0(7\ 3) \\
+) & -2\ 1\ 9 \quad [=(-3)\cdot 73] \\
\hline
& 8\ 9(0\ 1) \\
+) & -3 \quad [=(-3)\cdot 1] \\
\hline
& 8\ 6
\end{array}$$

因为 $86 \vdots 43$,所以 $912073 \vdots 43$.

例 4 判别 8962044 能否被 87 整除.

因为 $2\cdot10^3+1 \vdots 87$,就是 $k=3$, $M=-2$. 这就找到了判别法.我們挑其中的第二个方法来判别:

$$\begin{array}{rl}
8\ 9\ 6\ 2(0\ 4\ 4) & \\
+)\quad -8\ 8 & [=(-2)\cdot44] \\
\hline
8(8\ 7\ 4) & \\
+)\ -1\ 7\ 4\ 8 & [=(-2)\cdot874] \\
\hline
-1\ 7\ 4\ 0 &
\end{array}$$

于是我們只需判别 1740 能否被 87 整除(当然这是个容易檢驗的問題).

因为 $26\cdot10+1 \vdots 87$,就是 $k=1$, $M=-26$. 于是上面留下的問題,可以这样解决:

$$\begin{array}{rl}
1\ 7\ 4(0) & \\
+)\qquad 0 & [=(-26)\cdot0] \\
\hline
1\ 7(4) & \\
+)\ -1\ 0\ 4 & [=(-26)\cdot4] \\
\hline
-8\ 7 &
\end{array}$$

因为 $-87 \vdots 87$,就是 $1740 \vdots 87$. 从而 $8962044 \vdots 87$.

这条定理的第二个方法,可以叫做截尾法.

§3 D 是 $M_2\cdot10^k-M_1$ 的約数

我們已經看到上面两节里的定理所含內容非常丰富. 但是, 尽管如此, 这里还要介紹一条更加一般的定理——上面两条定理仅是它的推論.

定理 如果 $M_2 10^k-M_1 \vdots D$, D 是正整数, M_1、M_2 是非零整数①,且 $(|M_1|, |M_2|)=1$, 那末

① 如果 $M_2=1$, 那末,当 $M_1=0$ 的时候定理也成立.

(1) $N \vdots D \rightleftarrows A \vdots D$;

$[A = M_2^t A_{0(k)} + M_2^{t-1} M_1 A_{1(k)} + \cdots\cdots + M_2 M_1^{t-1} A_{t-1(k)} + M_1^t A_{t(k)}]$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A' = M_1 \overline{a_n \cdots\cdots a_k} + M_2 A_{0(k)}]$

証明(1) 由条件可知$(|M_2|, D)=1$. 因为，如果$(|M_2|, D)=d>1$，就导出$M_1 \vdots d$. 于是$(|M_1|, |M_2|)>1$.

因此$(|M_2^t|, D)=1$. 无疑的，$N \vdots D \rightleftarrows M_2^t N \vdots D$. 所以只需証明：$M_2^t N \vdots D \rightleftarrows A \vdots D$.

$$
\begin{aligned}
& M_2^t N - A \\
= & [M_2^t 10^{tk} A_{t(k)} + M_2^t 10^{(t-1)k} A_{t-1(k)} + \cdots\cdots + M_2^t 10^k A_{1(k)} + M_2^t A_{0(k)}] \\
& - [M_1^t A_{t(k)} + M_1^{t-1} M_2 A_{t-1(k)} + \cdots\cdots + M_1 M_2^{t-1} A_{1(k)} + M_2^t A_{0(k)}] \\
= & [(M_2 10^k)^t - M_1^t] A_{t(k)} + M_2[(M_2 10^k)^{t-1} - M_1^{t-1}] A_{t-1(k)} + \cdots\cdots \\
& + M_2^{t-1}[M_2 10^k - M_1] A_{1(k)}.
\end{aligned}
$$

显然，$M_2^t N - A \vdots M_2 10^k - M_1$，也就是$M_2^t N - A \vdots D$.

所以可以推得：$M_2^t N \vdots D \rightleftarrows A \vdots D$. 也就是說，$N \vdots D \rightleftarrows A \vdots D$.

(2) 因为$M_2 N \vdots D \rightleftarrows N \vdots D$. 于是只需証明：

$$M_2 N \vdots D \rightleftarrows A' \vdots D.$$

而 $M_2 N - A'$

$$
\begin{aligned}
& = [M_2 \cdot 10^k \overline{a_n \cdots\cdots a_k} + M_2 A_{0(k)}] - [M_1 \overline{a_n \cdots\cdots a_k} + M_2 A_{0(k)}] \\
& = (M_2 10^k - M_1) \overline{a_n \cdots\cdots a_k} \vdots M_2 10^k - M_1.
\end{aligned}
$$

就是$M_2 N - A' \vdots D$，所以可推得：$M_2 N \vdots D \rightleftarrows A' \vdots D$.

这一定理，如果$k=2$，$M_1=2$，$M_2=3$，就适用于$3 \cdot 10^2 - 2$（即$2 \cdot 149$）$\vdots D$的时候；

又如，$k=3$，$M_1=-3$，$M_2=2$，就适用于$2 \cdot 10^3 + 3$(即2003) $\vdots D$的时候；

又如，$k=3$，$M_1=5$，$M_2=4$，就适用于$4 \cdot 10^3 - 5$(即$5 \cdot 17 \cdot 47$) $\vdots D$的时候；

又如，$k=3$，$M_1=-2$，$M_2=4$，就适用于$4 \cdot 10^3 + 2$（$=2 \cdot 3 \cdot 23 \cdot 29$）$\vdots D$的时候；等等.

在具体应用定理之前，先把求 A 的运算安排如下，以便简捷地求出判别数。

数 $A=M_2^t A_{0(k)}+M_2^{t-1}M_1A_{1(k)}+\cdots\cdots+M_1^t A_{l(k)}$ 可由下法求出：

$$
\begin{array}{rl}
A_{0(k)} & (\cdot M_2) \\
+)\qquad\qquad A_{1(k)} & (\cdot M_1) \\
\hline
M_2A_{0(k)}+M_1A_{1(k)} & (\cdot M_2) \\
+)\qquad\qquad A_{2(k)} & (\cdot M_1^2) \\
\hline
\cdots\cdots\cdots\cdots\cdots\cdots & \\
+)\qquad\qquad A_{l(k)} & (\cdot M_1^t) \\
\hline
M_2^t A_{0(k)}+\cdots\cdots+M_1^t A_{l(k)} & =A
\end{array}
$$

数 A 也可由下法求出：

$$
\begin{array}{rl}
A_{l(k)} & (\cdot M_1) \\
+)\qquad\qquad A_{l-1(k)} & (\cdot M_2) \\
\hline
M_1A_{l(k)}+M_2A_{l-1(k)} & (\cdot M_1) \\
+)\qquad\qquad A_{l-2(k)} & (\cdot M_2^2) \\
\hline
\cdots\cdots\cdots\cdots\cdots\cdots & \\
+)\qquad\qquad A_{0(k)} & (\cdot M_2^t) \\
\hline
M_1^t A_{l(k)}+\cdots\cdots+M_2^t A_{0(k)} & =A
\end{array}
$$

至于数 $A'=M_1\overline{a_n\cdots\cdots a_k}+M_2A_{0(k)}$ 的求法很简单，这里可以从略.

例 1 判别 314539 能否被 149 整除.

因为 $3\cdot10^2-2 \vdots 149$，就是 $k=2$，$M_1=2$，$M_2=3$. 这就找到了判别法.

用第一个方法来判别：

$$
\begin{array}{rl}
3\ 9 & (\cdot 3) \\
+)\ \ 4\ 5 & (\cdot 2) \\
\hline
2\ 0\ 7 & (\cdot 3) \\
+)\ \ 3\ 1 & (\cdot 2^2) \\
\hline
7\ 4\ 5 &
\end{array}
$$

于是只需判别 745 能否被 149 整除.

$$\begin{array}{rl} 45 & (\cdot 3) \\ +)\quad 7 & (\cdot 2) \\ \hline 149 & \end{array}$$

由結果可以知道 745 ⋮ 149,从而 314539 ⋮ 149.

用第二个方法来判别:

$$\begin{array}{rl} 3145 & (\cdot 2) \\ +)\quad 39 & (\cdot 3) \\ \hline 6407 & \end{array}$$

于是只需判别 6407 能否被 149 整除. 这可以用同样方法处理:

$$\begin{array}{rl} 64 & (\cdot 2) \\ +)\quad 7 & (\cdot 3) \\ \hline 149 & \end{array}$$

由結果可以知道 6407 ⋮ 149,从而 314539 ⋮ 149.

对于 149, 当然还可以找到 $k=1$, $M_1=1$, $M_2=15$ (即 $15\cdot 10-1$ ⋮ 149)的判别法. 不过这由 § 2 的定理已可解决.

例 2 判别 3461255 能否被 799 整除.

(显然 $8\cdot 10^2-1$ ⋮ 799, 即 $k=2$, $M_1=1$, $M_2=8$, 不过这由 § 2 的定理已可以解决.)

因为 $4\cdot 10^3-5$ (即 3995) ⋮ 799, 就是 $k=3$, $M_1=5$, $M_2=4$. 这就找到了判别法.

用第一个方法来判别:

$$\begin{array}{rl} 255 & (\cdot 4) \\ +)\quad 461 & (\cdot 5) \\ \hline 3325 & (\cdot 4) \\ +)\quad 3 & (\cdot 5^2) \\ \hline 13375 & \end{array}$$

于是只需判别 13375 能否被 799 整除. 这就可以用同样方法来处理:

$$\begin{array}{rrl} & 375 & (\cdot 4) \\ +) & 13 & (\cdot 5) \\ \hline & 1565 & \end{array}$$

很容易看到 1565 不⋮799,所以 3461255 不⋮799.

用第二个方法来判别:

$$\begin{array}{rrl} & 3461 & (\cdot 5) \\ +) & 255 & (\cdot 4) \\ \hline & 18325 & \end{array}$$

下面继续判别 18325 能否被 799 整除.

$$\begin{array}{rrl} & 18 & (\cdot 5) \\ +) & 325 & (\cdot 4) \\ \hline & 1390 & \end{array}$$

因为 1390 不⋮799,就是 18325 不⋮799. 从而推知 3461255 不⋮799.

例 3 判别 755761 能否被 251 整除.

(因为 $10^3+4 \vdots 251$, 就是 $k=3$, $M_1=-4$, $M_2=1$. 这由 §1 的定理已可以解决.)

因为 $5\cdot10^2+2 \vdots 251$, 就是 $k=2$, $M_1=-2$, $M_2=5$. 这就找到了判别法:

用第一个方法来判别:

$$\begin{array}{rrl} & 61 & (\cdot 5) \\ +) & 57 & [\cdot(-2)] \\ \hline & 191 & (\cdot 5) \\ +) & 75 & [\cdot(-2)^2] \\ \hline & 1255 & \end{array}$$

然后判别 1255 能否被 251 整除.

$$\begin{array}{r} 5\ 5 \quad (\cdot 5) \\ +)\ 1\ 2 \quad [\cdot(-2)] \\ \hline 2\ 5\ 1 \end{array}$$

由結果可以知道 $1255 \vdots 251$，从而 $755761 \vdots 251$.

用第二个方法来判别：

$$\begin{array}{r} 7\ 5\ 5\ 7 \quad [\cdot(-2)] \\ +)\quad 6\ 1 \quad (\cdot 5) \\ \hline -1\ 4\ 8\ 0\ 9 \end{array}$$

然后判别 14809 能否被 251 整除.

$$\begin{array}{r} 1\ 4\ 8 \quad [\cdot(-2)] \\ +)\quad 9 \quad (\cdot 5) \\ \hline -2\ 5\ 1 \end{array}$$

由結果可以知道 $14809 \vdots 251$，从而 $755761 \vdots 251$.

至此，对于整除性的判别法問題，已相当完满的解决了．就是說：对于任意的除数 D，一定可以找到适宜的数組 k、M_1、M_2，使 $M_2 10^k - M_1 \vdots D$.

最后再举一个例子作为結束.

例 試作出对于 D（从 2—100）的整除性判别法.

对于 D，只要指出存在数組 k、M_1、M_2，使 $M_2 10^k - M_1 \vdots D$；这就是說，对于 D，存在整除性判别法.

无疑地，对于 D，适合于 $M_2 10^k - M_1 \vdots D$ 的 k、M_1、M_2 数組存在着无穷多个．下面所指出的数組都認为是比較适宜的.

D	使 $M_2 10^k - M_1 \vdots D$ 的数組 k、M_1、M_2
2	1, 0, 1
3	1, 1, 1
4	2, 0, 1; 1, 2, 1; 1, −2, 1
5	1, 0, 1
6	1, 4, 1; 1, −2, 1

D	使 $M_2 10^k - M_1 \vdots D$ 的数組 k、M_1、M_2
7	1, 3, 1; 1, −1, 2; 3, −1, 1
8	3, 0, 1; 1, 2, 1
9	1, 1, 1
10	1, 0, 1
11	1, −1, 1; 3, −1, 1
12	1, −2, 1
13	1, −3, 1; 1, 1, 4; 3, −1, 1; 2, −4, 1
14	1, −4, 1; 2, 2, 1
15	1, −5, 1
16	4, 0, 1; 2, 4, 1; 1, −2, 3
17	2, −2, 1; 1, −1, 5; 3, −3, 1
18	2, 10, 1; 1, −2, 7
19	1, 1, 2; 2, 5, 1; 2, 1, 4
20	2, 0, 1
21	1, −1, 2; 2, −5, 1; 4, 4, 1
22	2, −10, 1; 1, 8, 3; 2, −6, 5
23	1, 1, 7; 2, 1, 3; 3, −1, 2; 1, −3, 2
24	2, 4, 1; 1, 2, 5
25	2, 0, 1
26	2, −4, 1; 1, 4, 3; 1, −2, 5
27	3, 1, 1; 1, −1, 8; 2, −8, 1
28	4, 4, 1; 1, 2, 3
29	1, 1, 3; 3, −1, 2; 4, −5, 1
30	2, 10, 1
31	1, −1, 3; 3, 1, 4; 2, −3, 4
32	5, 0, 1; 2, 4, 1; 3, 8, 1; 1, −2, 3
33	2, 1, 1; 1, 7, 4
34	2, −2, 1; 1, −4, 3
35	2, −5, 1; 1, −5, 3
36	2, −8, 1; 1, −2, 7
37	3, 1, 1; 1, 3, 4
38	1, −8, 3; 2, −4, 3; 3, −2, 3
39	1, 1, 4

D	使 $M_2 10^k - M_1 \vdots D$ 的数組 k、M_1、M_2
40	3, 0, 1
41	1, −1, 4; 4, −4, 1
42	4, 4, 1; 3, −8, 1; 2, −4, 5
43	2, −1, 3; 3, 1, 4; 1, −3, 4
44	1, 6, 5; 1, 2, 9; 2, 12, 1; 2, −4, 7
45	1, −5, 4; 2, 10, 1
46	2, 8, 1; 1, 4, 5; 1, −2, 9; 2, −6, 5
47	2, 6, 1; 1, 3, 5
48	2, 4, 1; 3, −8, 1; 1, 2, 5
49	2, 2, 1; 1, 1, 5; 4, 4, 1
50	2, 0, 1
51	2, −2, 1; 1, −1, 5
52	2, −4, 1; 1, −2, 5
53	2, −6, 1; 1, −3, 5
54	2, −8, 1; 1, −4, 5
55	2, −10, 1; 1, 5, 6; 2, −5, 6
56	3, −8, 1; 1, −6, 5
57	2, 1, 4; 1, −7, 5
58	1, −8, 5; 2, 10, 3; 4, 4, 5
59	1, 1, 6; 3, −3, 1
60	1, 10, 7
61	1, −1, 6; 4, −4, 1; 2, −5, 3
62	1, 8, 7; 2, −10, 3; 3, 8, 1
63	3, −8, 1
64	6, 0, 1; 4, 2^4, 1; 1, 6, 7
65	1, −5, 6; 2, 5, 2
66	3, 10, 1; 1, 4, 7
67	2, −1, 2; 3, −5, 1; 1, 3, 7
68	4, 4, 1; 1, 2, 7
69	1, 1, 7; 4, −5, 1; 2, −7, 2
70	3, 20, 1; 3, −10, 3
71	1, −1, 7; 3, 6, 1; 2, 3, 5
72	3, −8, 1; 1, −2, 7

D	使 $M_2 10^k - M_1 \vdots D$ 的数組 k、M_1、M_2
73	4, −1, 1; 1, −3, 7; 2, 8, 3
74	4, 10, 1; 1, −4, 7; 2, 4, 3
75	1, −5, 7
76	1, −6, 7; 2, −4, 3; 3, 12, 1
77	3, −1, 1; 1, 3, 8; 2, −8, 3
78	1, −8, 7; 2, −2, 7
79	1, 1, 8; 3, −2, 3; 2, 5, 4
80	4, 0, 1; 1, −10, 7
81	1, −1, 8; 2, −5, 4
82	4, −4, 1; 2, 8, 5; 3, −2, 5
83	1, −3, 8; 3, 4, 1; 2, 2, 5
84	4, 4, 1; 3, −8, 1; 2, −4, 5
85	1, −5, 8; 2, 5, 6; 3, 5, 4
86	1, 4, 9
87	4, −5, 1; 3, −1, 2; 1, −7, 8
88	1, 2, 9; 2, −4, 7
89	1, 1, 9; 2, −1, 8
90	2, 10, 1; 3, 10, 1
91	1, −1, 9; 2, 9, 1; 3, −1, 1
92	2, 8, 1; 1, −2, 9
93	2, 7, 1; 3, 1, 4; 1, 7, 10
94	2, 6, 1; 1, −4, 9
95	2, 5, 1; 1, −5, 9
96	2, 4, 1
97	2, 3, 1
98	2, 2, 1
99	2, 1, 1
100	2, 0, 1

注 1 对于 D，究竟挑哪一組 k、M_1、M_2 較适宜，最好看 N 的位数多少再决定.

如果 N 的位数較多，可先挑出一个 k 值較大的数組 k、M_1、M_2 来用（这时 $|M_1|$、$|M_2|$ 的值应該选擇比較小的）. 这样，就可以把原来的整

除性判別問題迅速地归結成一个較簡单的整除性判別問題，就是N的位数比較少．这时我們可以再挑出一个k值較小的数組k、M_1、M_2（这时$|M_1|$、$|M_2|$即使稍大一点也无妨）来解决．

注2 如果$D=ab\cdots\cdots l$，而a，b，……，l这n个数是两两互质的，那末

$$N \vdots D \rightleftarrows N \vdots a,\ N \vdots b,\ \cdots\cdots,\ N \vdots l.$$

就是說，如果$N \vdots a$，$N \vdots b$，……，$N \vdots l$，那末$N \vdots D$；反过来，如果a，b，……，l中有一个数不能整除N，那末N不$\vdots D$．

例如，要判別N能否被63整除，只需判別N能否既被7整除又被9整除［这里$(7,9)=1$］．

例如要判別N能否被60整除，只需判別N能否被3、4、5整除（这里3、4、5两两互質）．

第三章 数的分解

要具体的进行数的分解，我們除已經具有了整除性的判別法外，还必須解决一个重要的理論問題——一个整数能唯一地表示成質数乘积的形式，这个定理也叫做算术基本定理．为了証明这个定理，当然应該做些准备工作，所以在一开始就把自然数分了类，継而討論了質数的一些性質．

除了上述的主要内容外，在本章中还介紹了約数的个数、約数之和两个公式．最后，特別地对于質数理論中的有趣問題作了簡单介紹．

§1 質数与合数．

不等于1的自然数，如果它只具有两个約数，就叫做質数（或素数）；如果具有两个以上的約数，就叫做合数．

定理 任何不是1的自然数，至少存在一个是質数的約数（質約数）．

証明 設自然数 $A\neq 1$.

(1) 如果 A 是质数，显然，A 的本身就是它的質約数，所以定理是成立的.

(2) 如果 A 是合数，由合数的定义可以知道，一定存在数 p_1，使 $A \vdots p_1$，而且 $A>p_1>1$.

如果 p_1 是质数，也就証明了定理的成立.

如果 p_1 是合数，由合数定义可以知道，一定存在数 p_2，使 $p_1 \vdots p_2$，而 $p_1>p_2>1$.

如果 p_2 是质数，因为 $A \vdots p_1$，而 $p_1 \vdots p_2$，就得到 $A \vdots p_2$. 所以这时定理也就成立了.

如果 p_2 是合数，又由合数定义可以知道，一定存在数 p_3，使 $p_2 \vdots p_3$，而 $p_2>p_3>1$.

繼續研究下去，可得到一連串的数：p_1、p_2、p_3、……，而它們之間存在着如下的关系：$p_1>p_2>p_3>\cdots\cdots>1$.

显然，这是一个有限数列. 設末項是 p_n，那末 p_n 一定是质数（如果 p_n 是合数，一定存在数 p_{n+1} 使 $p_n \vdots p_{n+1}$，这样 p_n 就不是末項了）.

因此任意的一个不是 1 的自然数至少存在一个质約数.

§2 质数与合数的个数

容易知道，在自然数中合数的个数是无限多的，因为合数的任意一个倍数总是合数.

关于质数的个数問題，有如下的一个定理.

定理 在自然数中质数的个数无限多.

証明 設质数仅是有限个，由小到大依次排列如下：

$$2、3、5、\cdots\cdots、p.$$

我們只要証明除上述的这些质数外，另外还有质数就成了.

假定組成一个数 $N=2\cdot3\cdot5\cdots\cdots p+1$.

(1) 如果 N 本身就是质数，那末 $N>p$. 所以定理就成立.

(2) 如果N是合数，由上节知道N一定有質約数．現在分别以 2、3、5、……、p去除 N，都不能整除 N．这就說明合数 N 在这些質数內找不到它的約数，也就是在 2、3、5、……、p 这些質数之外还存在着新的質数．这样，定理也就被証实了．

注意 不要以为这样組成的数N一定是質数．例如，$2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031=59\cdot509$；又如，$2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17+1=510511=19\cdot97\cdot277$．

对于这个定理，我們如果按照下面的法則組成一个数N也可以得到証实：

如果質数是有限个，我們把这些个質数，任意的分做两类．譬如一类是：p_1、p_2、……、p_m；而另一类是：q_1、q_2、……、q_n．

假定把这些个質数来組成数 $N=(p_1p_2\cdots\cdots p_m)+(q_1q_2\cdots\cdots q_n)$．

如果N本身是質数，这时N当然是大于这些質数中的任何一个数，因而定理是成立了．

如果N是合数，已知它存在質約数．可是这些質数中的任何一个数都不能整除它(能整除其中的一項，但不能整除另一項)．这就証明了，在这些質数之外还有着新的質数．

提到質数个数的无限多問題，值得介紹一条有关的重要定理(尽管这里无法作出它的証明)．19 世紀的德国数学家狄里克萊 (Dirichlet) 証明了：如果 a、b 是互質数，那末当 n 取一切自然数时，形如 $an+b$ 的数中，包含着无限个質数．

我們这里只能对其中最簡单的特殊情形加以探討．譬如下面我們証明：当 n 取过一切自然数时，形如 $4n+3$ 的数中，包含着无限个質数．因为形如 $4n+3$ 的数，一定可以写成形如 $4n-1$ 的数．因此也就是說，形如 $4n-1$ 的数中包含着无限个質数．

在証明之前，应該了解下面的知識：

“一切大于 2 的質数，不是形如 $4n+1$，就是形如 $4n-1$．”

理由很簡单，因为大于 2 的質数当然是奇数，对于奇数难道可能是

形如 $4n$ 或者 $4n+2$ 的嗎？

"由形如 $4n+1$ 的数相乘，所得的乘积一定是形如 $4n+1$ 的数"。

这只要注意下面两个数的情形就够了：

$$(4a+1)(4b+1)=16ab+4a+4b+1=4(4ab+a+b)+1.$$

这样我們可以开始証明上述的定理了．

假定形如 $4n-1$ 的数中只含着有限个质数：p_1、p_2、……、p_k，我們用这些质数組成一个数 $N=4(p_1p_2\cdots p_k)-1$.

如果 N 是质数，定理显然成立．因为这时 N 本身就呈現出 $4n-1$ 的形状，且 N 比 p_1、p_2、……、p_k 中任何一个都大，这就否定了上面的假設．

如果 N 是合数，我們可以断定它的所有的质約数不能都呈現 $4n+1$ 的形状．因为如果所有的质約数都呈这个形状，它們的乘积① N 当然也应呈現这种形状．事实上，N 并不是这种形状．

就是說 N 一定有着形如 $4n-1$ 的质約数 p（因大于 2 的质数，不是形如 $4n+1$，就是形如 $4n-1$）．

容易看出形如 $4n-1$ 的质数 p 不会与 p_1、p_2、……、p_k 中的任何一个相等．因为 p_1、p_2、……、p_k 中任何一个都不是 N 的約数．这就表明除 p_1、p_2、……、p_k 外还存在着形如 $4n-1$ 的质数．这也就否定了上面的假設．

綜上所述，也就是証明了形如 $4n-1$ 的数中包含着无限多个质数．

讀者可以考虑"形如 $6n+5$ 的数（即形如 $6n-1$ 的数）中包含着无限多个质数"的証明．

关于自然数中的质数分布問題，讀者在这一章的最后，还有机会了解到一些．

§3 质数的檢定法和质数表的造法

判别一个数 N 是合数还是质数的方法，很明显，只要看小于 N 而大

① "合数可用质数的乘积来表示，"这一断言虽然在后面才提到，但是可以借来先用，因为它由 §1 的結果直接可推出．

1的一切自然数内是否有N的約数（当然可以把这些自然数依次的去試除N）. 这些自然数内有質数也有合数，但这些合数都有它們的質約数，而如果一个合数能整除数N，它的質約数就一定也能整除数N. 所以可把上述的判别法改成：如果小于N的一切質数都不能整除N，那末N是質数.

实际上，判别的方法可以更简单些.

定理 一数被小于它的一切質数由小到大的依次去試除，直到某一个質数去除它而所得到的商等于或开始小于該質数时还不能整除，那末这个数是質数. 也就是：

設 p_1、p_2、……、p_n 是小于N的由小到大的一切質数. 如果对于 $m=1$、2、3、……、$k-1$ ($k-1<n$)，下式都能成立：$N=p_mq_m+r_m$ ($0<r_m<p_m$)，且 $p_m<q_m$；但是当 $N=p_kq_k+r_k$ ($0<r_k<p_k$) 的时候，$p_k\geqslant q_k$，那末N是質数.

証明 題設 p_1，p_2、……、p_{k-1}、p_k 都不能整除N. 如果 $k<n$①，要証明N是質数，就需証明N也不能被 p_{k+1}、p_{k+2}、……、p_n 所整除.

如果 p_t ($k+1\leqslant t\leqslant n$) 能整除$N$，設 $N=p_t\cdot q$. 因为 $p_t\geqslant p_{k+1}>p_k$，可以断定 $q<p_k$ [不然，如果 $q\geqslant p_k$，由 $p_t\geqslant p_{k+1}\geqslant p_k+1$，可得：$N=p_t\cdot q\geqslant(p_k+1)\cdot p_k$. 因为 $p_k\geqslant q_k$，所以 $N\geqslant(q_k+1)\cdot p_k$. 但是已知 $N=p_kq_k+r_k$ ($0<r_k<p_k$)，那末$N<(q_k+1)\cdot p_k$. 矛盾是由所設 $q\geqslant p_k$ 而引起的]. 所以 q 的質約数一定在 p_1、p、……、p_{k-1} 之中. 由$N=p_t\cdot q$，知 $N \vdots q$，当然在 p_1、p_2、……、p_{k-1} 之中而属于 q 的約数的数也能整除N. 但由題設可知 p_1、p_2、……、p_{k-1} 中的任何一个数都不能整除 N，显然，p_t 不能整除N，也就証明了N是質数.

例 判别 487 是不是質数.

我們用質数 2、3、5、……依次地去除 487，直到用 23 去除得到不完全商 21，而还不能整除，于是就肯定 487 这个数是質数.

关于判别質数，也可以根据如下的形式上或許更簡单的定理：如果

① 如果 $k=n$，那末“N 是質数”就不需要証明了.

一切不大于$\sqrt{N}$的质数中沒有一个是N的約数，那末N一定是个質数.

它的根据与上述沒有多大差別，因此把証明省略了.

如上例的数 487．不大于$\sqrt{487}$的质数是 2、3、5、……、19．可是用这些質数依次地去試除 487 都不能整除．也就是說，这些質数都不是 487 的約数，所以 487 是質数.

下面轉入造質数表問題的討論.

爱拉托斯散納(Eratosthenes)的篩子:

爱氏是用这样的方法找出自然数N以内的一切質数的，就是把N以内的所有合数都篩去.

把N以内的自然数(1除外)按次序排列：2、3、4、5、……、N.

第一个的 2 是質数，我們按次地从这些数内把在 2 以后的所有 2 的倍数都划掉(如 4、6、8、……).

2 后面的 3 沒有被划掉，这就說明它不是 2 的倍数，它只有两个約数(1 与 3)，所以 3 也是質数．把 3 留下，再按次地从这些数内划掉在 3 以后的所有 3 的倍数(如 6、9、12、……)，当然其中有些数在划掉 2 的倍数时已被划去了．在 3 的后面沒有被划去的是 5，可見 5 不是 2 或 3 的倍数(不然早該划去了)，就是 5 只有两个約数(1 与 5)，所以 5 也是質数．同样的，我們在 5 的后面划去所有的 5 的倍数.

这样繼續下去，直到N以内的数沒有再能被划去的，那末这些留下来的数就是N以内的一切質数.

譬如下面我們先来造一个 100 以内的質数表：先按次序地写出 2 到 100 的自然数.

留下質数 2，划去后面所有 2 的倍数．2 后面的数 3 是質数，我們再划去 3 后面的所有 3 的倍数．与上面已經說过的一样，再划去 5 后面所有 5 的倍数．5 后面未被划掉的是 7，显然，7 不是 2、3、5 的倍数(不然的話，早該划掉了)；当然不会是 4、6 的倍数．这样，7 就只有两个約数，也就是說，它是个質数．以后我們再划去 7 后面的所有的 7 的倍数.

7 的后面未被划掉的是 11，照例应該划去 11 后面的所有的 11 的

倍数，然而在100以内的那些数早在以前就陆續的被划掉了(那些数不是2的倍数就是3、5、7中某一个的倍数)．因此对于“划”的工作可以不再継續了，那些留下来的数就是100以内的所有的質数．

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

一般的，造一个在已知数N以内的質数表，可根据如下的定理：

定理　設不大于$\sqrt{N}$的从小到大的質数是：2、3、5、……、p.在自然数2—N中，依次地划去2、3、5、……、p以外的所有它們的倍数，那末所留下来的数就是在N以内的一切質数．

証明　2、3、5、……、p这些数也是留下来的，它們当然是質数，我們要証明留下的数中除这些数以外也都是質数．

在那些数里我們只要任意的挑出一个数(設为m)来加以观察就够了．要証明m是質数，已經知道只需証明：一切不大于$\sqrt{m}$的質数中沒有一个是m的約数．关于这一点是很容易証明的．因为$m \leqslant N$，而2、3、5、……、p是一切不大于$\sqrt{N}$的質数，所以一切不大于$\sqrt{m}$的質数的个数总不会比2、3、5、……、p这些个質数更多．然而在2、3、5、……、p中的任何一个都不是m的約数(不然，数m早該被划去了)．于是証明了m是質数．

譬如，前面我們造过在100以内的質数表．因为不大于$\sqrt{100}$的一切質数是2、3、5、7，所以只要划去2、3、5、7以外的所有它們的倍数就成了．又如，我們如果要造1000以内的質数表，就只需如下做去：因为不大于$\sqrt{1000}$的一切質数是：2、3、5、7、11、17、19、23、29、31，所以只需划去除它們之外的所有它們的倍数就成了．

关于質数表，据說愛氏自己只造了一个1000以内的．到17世紀，

不过出現了一个一万以內的質数表，以后才出現了比較完备的質数表．現在可以找到的最完备的質数表是从 1 到 10,006,721．

§4 数的分解

要解决数的分解問題，必須先掌握下面的两条定理．

定理 任何一个合数都能用質数的乘积来表示．

証明 設 N 是合数，由 §1 的定理可知它一定有質約数．設 p_1 是 N 的質約数，那末 $N=p_1N_1$．

如果 N_1 是質数，定理就获得証实．

如果 N_1 是合数，当然它一定有質約数，設質約数是 p_2，那末 $N_1=p_2N_2$．于是得 $N=p_1p_2N_2$．

如果 N_2 是質数，定理也就获得証实．

如果 N_2 是合数，同理它有質約数 p_3，……这样繼續下去，可得出数列：

$$N,\ N_1,\ N_2,\ N_3,\ \cdots\cdots.$$

这个数列中的每一个数都大于 1，而且

$$N>N_1>N_2>N_3>\cdots\cdots.$$

因为 N、N_1、N_2、…… 都是自然数，所以該数列的項数不可能是无限的．設 N_m 是該数列的末項，那末 N_m 一定是質数（不然，由上面所述可知还存在 N_{m+1}，这样 N_m 就不是末項了）．于是

$$N=p_1N_1=p_1p_2N_2=\cdots\cdots=p_1p_2p_3\cdots\cdots p_{m-1}p_mN_m.$$

这就是說，任何一个合数一定可以用質数的乘积来表示．

定理 一个合数只能用唯一的質数乘积来表示．

証明 設 $N=a_1a_2a_3\cdots\cdots a_m$（这 m 个数 a_1、a_2、……、a_m 都是質数，这些数中的任意两个也可能相等）；$N=b_1b_2b_3\cdots\cdots b_n$（这 n 个数 b_1、b_2、……、b_n 都是質数，这些数中的任意两个也可能相等）．

我們要証明：a_1、a_2、a_3、……、a_m 与 b_1、b_2、b_3、……、b_n 除書写次序可能不同外是完全一致的．

因为　$a_1a_2\cdots\cdots a_m=b_1b_2\cdots\cdots b_n$，

所以　$a_1a_2\cdots\cdots a_m \vdots b_s$。$(1\leqslant s\leqslant n)$

于是可断言乘积中一定有一个因数与 b_s 相等．因为如果沒有一个因数与 b_s 相等，也就是 $(a_i, b_s)=1$ $(i=1、2、3、\cdots\cdots、m)$．因此 $(a_1a_2\cdots\cdots a_m, b_s)=1$．这个結論与 $a_1a_2\cdots\cdots a_m \vdots b_s$ 是矛盾的．

設 $a_t=b_s$ $(1\leqslant t\leqslant m)$，于是

$$a_1a_2\cdots\cdots a_{t-1}a_{t+1}\cdots\cdots a_m=b_1b_2\cdots\cdots b_{s-1}b_{s+1}\cdots\cdots b_n.$$

如果在上式右边再任挑一个因素 $b_{s'}$，同理，在左边一定有因素 $a_{t'}$ 与它相等．

按照这样繼續下去，就証明了：对于任意一个 b_j $(j=1、2、\cdots\cdots、n)$，一定可以在乘积 $a_1a_2\cdots\cdots a_m$ 中找到一个因数与它相等．

按照同样的步驟，可以証明：对于任意一个 a_i $(i=1、2、\cdots\cdots、m)$，一定可以在乘积 $b_1b_2\cdots\cdots b_n$ 中找到一个因数与它相等．

綜上所述，可知 a_1、a_2、$\cdots\cdots$、a_m 与 b_1、b_2、$\cdots\cdots$、b_n 除書写次序可能不同外，是完全一致的．这就証明了合数 N 只能用唯一的質数乘积来表示．

如果在質数的乘积中考慮到質数由小到大的次序，以及相同数連乘写成冪的形式，那末合数用質数乘积表示可以写成如下的形式：

$$N=p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}\cdots\cdots p_n^{\alpha_n}.$$

这里 p_1、p_2、p_3、$\cdots\cdots$、p_n 是相异的質数，且

$$p_1<p_2<p_3<\cdots\cdots<p_n.$$

例　如果正整数 M、N 不能以同底数的冪表示（底数与冪指数指的是正整数），那末对数 $\log_M N$ 一定是无理数．

証明　如果 $\log_M N=\dfrac{p}{q}$ [p、q 是正整数，且 $(p, q)=1$]，由对数的定义可知：$M^{\frac{p}{q}}=N$；也就是 $M^p=N^q$．　　　(1)

設 $M=a_1^{\alpha_1}a_2^{\alpha_2}\cdots\cdots a_m^{\alpha_m}$，$N=b_1^{\beta_1}b_2^{\beta_2}\cdots\cdots b_n^{\beta_n}$

（a_1、a_2、$\cdots\cdots$、a_m 是相异的質数，且 $a_k<a_{k+1}$．

b_1、b_2、……、b_n 也是相异的质数，且 $b_k<b_{k+1}$)。

代入(1)得：　$a_1^{\alpha_1 p}a_2^{\alpha_2 p}\cdots\cdots a_m^{\alpha_m p}=b_1^{\beta_1 q}b_2^{\beta_2 q}\cdots\cdots b_n^{\beta_n q}$.

既然一个数只能用唯一的质数乘积形式来表示，所以这里 $m=n$，且 $a_i=b_i$，$\alpha_i p=\beta_i q$ ($i=1$、2、……、n)。于是$\frac{\alpha_i}{\beta_i}=\frac{q}{p}$. 因为 $(p, q)=1$，所以 $\alpha_i=A_i q$，$\beta_i=A_i p$ (A_i 是 正整数)。

这样，$M=a_1^{A_1 q}a_2^{A_2 q}\cdots\cdots a_n^{A_n q}=(a_1^{A_1}a_2^{A_2}\cdots\cdots a_n^{A_n})^q$,

$$N=b_1^{A_1 p}b_2^{A_2 p}\cdots\cdots b_n^{A_n p}=(b_1^{A_1}b_2^{A_2}\cdots\cdots b_n^{A_n})^p.$$

因为 $a_i=b_i$，于是 $a_i^{A_i}=b_i^{A_i}$. 也就是說，

$$a_1^{A_1}a_2^{A_2}\cdots\cdots a_n^{A_n}=b_1^{A_1}b_2^{A_2}\cdots\cdots b_n^{A_n}=S.$$

于是 $M=s^q$，$N=s^p$.这就是說 M、N 能用同底数的冪表示. 显然，这与題設矛盾，于是証明了对数 $\log_M N$ 应是无理数.

反过来，如果 M、N 能用同底数的冪表示，那末 $\log_M N$ 一定是有理数.

理由极明显，可以从略。

譬如，$\log_2 5$、$\log_{10} 8$、$\log_{16} 24$ 等等都是无理数；$\log_2 8$、$\log_{27} 81$ 等等都是有理数.

由上面的两条定理，我們知道了一个合数可以用质数乘积的形式来表示，而且这种形式是唯一的.下面我們来討論如何把一个合数用质数乘积的形式来表示.

把一个合数表示成质数乘积的形式，叫做数的质因数分解.对于一个数的质因数分解的方法如下：

$$\begin{array}{r|l} p_1 & N \\ \hline p_2 & N_1 \\ \hline p_3 & N_2 \\ \hline \cdots\cdots & \\ p_n & N_{n-1} \\ \hline & N_n \end{array}$$

我們按次地用由小到大的质数去試除N（可以应用学过的整除性的判别法）.

設质数 p_1 能整除 N，商是 N_1；如果 N_1 不是质数，又設质数 p_2 能整除 N_1，而商是 N_2；如果 N_2 又不是质数，再設质数 p_3 能整除 N_2，这样繼續下去.

設质数 p_n 能整除 N_{n-1}，而商 N_n 是质数. 于是得

到的 p_1、p_2、p_3、……、p_n、N_n 都是N的質約数，而

$$N=p_1N_1=p_1p_2N_2=\cdots\cdots=p_1p_2p_3\cdots\cdots p_nN_n.$$

(可写成$N=q_1^{\alpha_1}q_2^{\alpha_2}\cdots\cdots q_n^{\alpha_n}$ 的形式)

在习惯上，为了便利起見，我們取的 p_1 是N的最小的質約数；p_2 是 N_1 的最小的質約数，一般的，p_k 是 N_{k-1} 的最小的質約数.

如果 p_{k+1} 是 N_k 的質約数，而 N_k 当然是 N_{k-1} 的約数，所以推得 p_{k+1} 也是 N_{k-1} 的質約数.已知 p_k 是 N_{k-1} 的最小質約数，所以 $p_k\leqslant p_{k+1}$.

这也就是說，所得到的質約数 p_1、p_2、……、p_n 之間有着下列关系：$p_1\leqslant p_2\leqslant\cdots\cdots\leqslant p_n$.

例 把 750750 分解質因数.

2	750750
3	375375
5	125125
5	25025
5	5005
7	1001
11	143
	13

由左边的算草，得

$$750750=2\cdot3\cdot5\cdot5\cdot5\cdot7\cdot11\cdot13$$
$$=2\cdot3\cdot5^3\cdot7\cdot11\cdot13.$$

有时为了方便起見，可先把一合数写成为几个較簡单的合数的乘积，然后再把几个合数分别地进行質因数分解.

例 把 16500 表示成質数的乘积.

因为 $16500=165\cdot100,$

而 $165=3\cdot5\cdot11,\quad 100=2^2\cdot5^2,$

所以 $16500=2^2\cdot3\cdot5^3\cdot11.$

§5 自然数的約数的个数

为了討論自然数N的約数个数問題，我們先来注意一条定理：

設N用質因数乘积形式表示如下：$N=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n}$.

那末 d 是 N 的約数的充分而且必要条件是:

$$d=p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}.$$

这里 $0\leqslant\beta_1\leqslant\alpha_1$, $0\leqslant\beta_2\leqslant\alpha_2$, ……, $0\leqslant\beta_n\leqslant\alpha_n$.

証明 关于条件的充分性的成立是极明显的.

因为如果 $d=q_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$ ($0\leqslant\beta_1\leqslant\alpha_1$, $0\leqslant\beta_2\leqslant\alpha_2$, ……, $0\leqslant\beta_n\leqslant\alpha_n$), 那末 $N \vdots d$.

下面我們証明条件的必要性的成立:

設 N 的約数 $d=p_1^{\gamma_1}q_2^{\gamma_2}\cdots\cdots q_m^{\gamma_m}$($q_1$、$q_2$、……、$q_m$ 是相异的質数).

我們只要証明对于 $q_1^{\gamma_1}$、$q_2^{\gamma_2}$、……、$q_m^{\gamma_m}$ 中的任意一个 $q_K^{\gamma_K}$, 在 $p_1^{\alpha_1}$、$p_2^{\alpha_2}$、……、$p_n^{\alpha_n}$ 中一定能找到一个数, 譬如是 $p_R^{\alpha_R}$, 而 $p_R=q_K$ 及 $\alpha_R\geqslant\gamma_K$.

因为 $d \vdots q_K^{\gamma_K}$, 又因为 $N \vdots d$, 所以 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n} \vdots q_K^{\gamma_K}$. (1)

如果質数 p_1、p_2, ……、p_n 中沒有一个与 q_K 相等, 那末 $(p_1, q_K)=1$, $(p_2, q_K)=1$, ……, $(p_n, q_K)=1$. 于是:

$$(p_1^{\alpha_1}, q_K^{\gamma_K})=1,\ (p_2^{\alpha_2}, q_K^{\gamma_K})=1,\ \cdots\cdots,\ (p_n^{\alpha_n}, q_K^{\gamma_K})=1.$$

所以 $$(p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n}, q_K^{\gamma_K})=1.$$

这个結論与(1)是矛盾的. 所以說在質数 p_1、p_2、……、p_n 中一定能找到一个数, 設 p_R 等于 q_K.

这样, 在相异質数 p_1、p_2、……、p_n 中除 p_R 外, 其余的就都与 q_K 互質. 就可以推得在数 $p_1^{\alpha_1}$、$p_2^{\alpha_2}$、……、$p_n^{\alpha_n}$ 中除 $p_R^{\alpha_R}$ 外, 其余的都与 $q_K^{\gamma_K}$ 互質. 从而推得除 $p_R^{\alpha_R}$ 外所有其余的数的乘积也与 $q_K^{\gamma_K}$ 互質.

把(1)的被除数改写做: $p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n}=p_R^{\alpha_R}\cdot M$.

由(1)知 $p_R^{\alpha_R}\cdot M \vdots q_K^{\gamma_K}$. 上面已指出过 $(M, q_K^{\gamma_K})=1$, 所以說, $p_R^{\alpha_R} \vdots q_K^{\gamma_K}$ [根据第一章 §3(11)推論 3].

因为 $p_R=q_K$, 于是得 $p_R^{\alpha_R} \vdots p_R^{\gamma_K}$. 所以 $\alpha_R\geqslant\gamma_K$.

这样, 就証明了条件的必要性. 也就是証明了 N 的約数 d 必具有下面的形式:

$$p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$$

$$(0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \cdots\cdots,\ 0\leqslant\beta_n\leqslant\alpha_n).$$

下面进一步討論自然数的約数个数問題.

自然数1,約数只有一个.任何質数，按它的定义可以知道有也只有两个約数.

因此我們主要是研究合数的約数个数問題.

定理 設自然数 $N=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n}$，那末 N 的約数的个数是:

$$(\alpha_1+1)(\alpha_2+1)\cdots\cdots(\alpha_n+1).$$

証明

在 p_1^0、p_1^1、p_1^2、……、$p_1^{\alpha_1}$ 这 α_1+1 个数中，任意取一个 $p_1^{\beta_1}$（当然 $0\leqslant\beta_1\leqslant\alpha_1$）;

在 p_2^0、p_2^1、p_2^2、……、$p_2^{\alpha_2}$ 这 α_2+1 个数中,任意取一个 $p_2^{\beta_2}$（当然 $0\leqslant\beta_2\leqslant\alpha_2$）;

………………………………………………;

在 p_n^0、p_n^1、p_n^2、……、$p_n^{\alpha_n}$ 这 α_n+1 个数中,任意取一个 $p_n^{\beta_n}$（当然 $0\leqslant\beta_n\leqslant\alpha_n$）.

上面已經証明过：乘积 $p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$ 一定是 N 的約数；反过来，N 的約数也一定具有这种形式.

观察乘积 $p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$ 的构成,我們知道它是分别从 α_1+1 个数中，α_2+1 个数中，……，α_n+1 个数中任意取一个数，連乘而得到的.所以形状如 $p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$ 的数，它的个数是:

$$(\alpha_1+1)(\alpha_2+1)\cdots\cdots(\alpha_n+1).$$

并且这許多个形状如 $p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$ 的数中不会有两个具有相同的数值.理由如下:

因为一个数用質数乘积表示的形式是唯一的.也就是說,不可能有这种情形：$p_1^{R_1}p_2^{R_2}\cdots\cdots p_n^{R_n}=p_1^{K_1}p_2^{K_2}\cdots\cdots p_n^{K_n}$. 而且 R_1，K_1；R_2，K_2；……；R_n，K_n；各对数中至少有一对是不相等的.

这样,就証明了 N 的約数个数是:

$$(\alpha_1+1)(\alpha_2+1)\cdots\cdots(\alpha_n+1).$$

如果我們以符号 $F(N)$ 表示数 N 的約数的个数，又假定我們熟悉

乘积的記号"Π". 这样就可以把定理縮写成:

$$F(N)=\prod_{K=1}^{n}(\alpha_K+1).$$

例 1 求 968 的約数的个数.

因为 $968=2^3\cdot 11^2$, 所以 968 的約数的个数是:

$$(3+1)(2+1)=4\cdot 3=12.$$

例 2 求 750750 的約数的个数.

因为 $750750=2\cdot 3\cdot 5^3\cdot 7\cdot 11\cdot 13$, 所以 750750 的約数个数是:

$$(1+1)(1+1)(3+1)(1+1)(1+1)(1+1)=128.$$

§6 自然数的約数的总和

設 $N=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n}$. (我們早就习惯了用 p_1、p_2、……、p_n 来表示相异的質数.)

观察乘积:

$(p_1^0+p_1^1+p_1^2+\cdots\cdots+p_1^{\alpha_1})(p_2^0+p_2^1+p_2^2+\cdots\cdots+p_2^{\alpha_2})\cdots\cdots$ $\cdots\cdots(p_n^0+p_n^1+p_n^2+\cdots\cdots+p_n^{\alpha_n})$. 容易看到, 如果把它展开, 就得到 $\prod\limits_{K=1}^{n}(\alpha_K+1)$ 个数的和, 而每个数都具有形式: $p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}$

$$(0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \cdots\cdots,\ 0\leqslant\beta_n\leqslant\alpha_n).$$

这就說明了該乘积是表示 N 的所有約数的和. 我們用符号 $S(N)$ 表示 N 的所有約数的和, 那末

$$S(N)=(p_1^0+p_1^1+\cdots\cdots+p_1^{\alpha_1})(p_2^0+p_2^1+\cdots\cdots+p_2^{\alpha_2})\cdots\cdots$$
$$\cdots\cdots(p_n^0+p_n^1+\cdots\cdots+p_n^{\alpha_n}).$$

下面我們設法簡化公式:

設 $S_i=p_i^0+p_i^1+p_i^2+\cdots\cdots+p_i^{\alpha_i}$, 根据等比数列求和公式可知:

$$S_i=\frac{p_i^{\alpha_i+1}-1}{p_i-1}.$$

所以 $S(N)=S_1S_2\cdots\cdots S_n$

$$=\left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\cdots\cdots\left(\frac{p_n^{\alpha_n+1}-1}{p_n-1}\right)$$

$$=\prod_{i=1}^{n}\left(\frac{p_i^{\alpha_i+1}-1}{p_i-1}\right).$$

例 1 求 11025 的一切約数的总和.

因为 $11025=3^2\cdot5^2\cdot7^2$，所以 11025 的所有約数的总和是：

$$\left(\frac{3^{2+1}-1}{3-1}\right)\left(\frac{5^{2+1}-1}{5-1}\right)\left(\frac{7^{2+1}-1}{7-1}\right)$$

$$=13\cdot31\cdot57=22971.$$

例 2 求 16500 的所有約数的总和.

因为 $16500=2^2\cdot3\cdot5^3\cdot11$，而

$$\left(\frac{2^3-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^4-1}{5-1}\right)\left(\frac{11^2-1}{11-1}\right)$$

$$=7\cdot4\cdot156\cdot12=52416.$$

所以 16500 的約数的和是 52416.

§7 质数理論中的几个有趣問題

所謂质数理論中的一些有趣問題，恰恰是一些最艰难的問題，当然这里只允許作一些略述.

先提一个完全数問題：

一个数如果等于除去它本身以外的一切約数的和，那末这叫做完全数.

例如，数 6 除去本身外的一切約数是 1、2、3，而 $6=1+2+3$，所以数 6 叫做完全数.

又如，数 28 除去本身外的一切約数是 1、2、4、7、14，而 $28=1+2+4+7+14$，所以 28 也叫完全数.

設 $S(N)$ 表示 N 的一切約数的和，显然，如果 $S(N)-N=N$，也

就是当 $N=\frac{1}{2}S(N)$时，N 是完全数.

欧几里德在他的“几何原本”中，对于完全数曾給出如下的一条定理：

如果 $m=2^p-1$ 是質数，那末 $2^{p-1}\cdot m$ 是完全数.

証明 設 $N=2^{p-1}\cdot m$，由条件知道 m 是質数，根据約数的总和公式可得：

$$S(N)=\left(\frac{2^{(p-1)+1}-1}{2-1}\right)\left(\frac{m^2-1}{m-1}\right)$$

$$=(2^p-1)(m+1)=m\cdot 2^p.$$

$$\therefore\quad N=2^{p-1}\cdot m=\frac{1}{2}\cdot 2^p\cdot m=\frac{1}{2}S(N).$$

这就証明了 N 是完全数.

显然，按照欧几里德的定理，如果要求得一个完全数(实际是偶完全数)，就必須求得数 p，使 2^p-1 是質数. 因此必須研究当 p 是怎样的数值时，2^p-1 是質数.

十七世紀的数学家梅爽(Mersenne)最先研究了这个問題，我們就把形如 2^p-1 的質数叫做梅爽数.

很明显，求得梅爽数的必要条件是 p 应为質数. 事实上，如果 $p=mn$ (m 和 n 都大于 1)，那末

$$2^p-1=2^{mn}-1$$

$$=(2^m-1)[2^{m(n-1)}+2^{m(n-2)}+\cdots\cdots+1].$$

显然，这时 2^p-1 就不是質数.

当然，p 是質数并非求得梅爽数的充分条件. 换句話說，并非只要 p 是質数，就可以求得梅爽数. 譬如，当 $p=11$ 时，$2^{11}-1=23\cdot 89$，而 $2^{11}-1$ 就不是質数.

到今天我們只发現了当 p 分别等于 2、3、5、7、13、17、19、31、61、89、107、127、521、607、1279、2203、2281 这十七个質数时，可得到梅爽数.

例如，$2^{127}-1=170141183460469231731687303715884105727$，是一个 39 位的质数．

又如，$2^{2281}-1$ 是一个 687 位的质数，这也是今天所知道的一个最大的质数．

对完全数問題来說，也就是到今天只发現了 17 个偶完全数．至于是否有无穷个偶完全数存在（即是否有无穷个梅爽数存在），以及是否可以找到奇完全数，这些問題尙待数学家們的研究．

下面介紹的問題，是与“尺規等分圓周問題（或尺規作正多边形）”这一著名的几何問題联系着的．

我們知道，如果用尺規可以 n 等分圓周，那末也一定可以用尺規把圓周等分成 2^kn（k 是非負整数）等分．

另外，設 $n=n_1n_2$，而 $(n_1, n_2)=1$，如果用尺規可以把圓周等分成 n_1 和 n_2 等份，那末用尺規也一定可以把圓周 n 等分．理由如下：

因为 $(n_1, n_2)=1$，所以可以选擇一对整数 x、y①，使满足等式：

$$n_1x+n_2y=1.$$

于是
$$\frac{y}{n_1}+\frac{x}{n_2}=\frac{1}{n}.$$

这就是說，只要知道圓周的 $\frac{1}{n_1}$ 部分和 $\frac{1}{n_2}$ 部分，就可以求得圓周的 $\frac{1}{n}$ 部分，从而就完成了 n 等分圓周的問題．

反过来，很明显，如果用尺規可以 2^kn 等分圓周，那末一定可以 n 等分圓周．

設 $n=n_1n_2$，而用尺規可以 n 等分圓周，那末一定能 n_1（或 n_2）等分圓周．理由如下：

因为已知圓周的 $\frac{1}{n}$ 部分，只要把圓周的 $\frac{1}{n}$ 部分重复 n_2（或 n_1）次就得到了圓周的 $\frac{1}{n_1}$（或 $\frac{1}{n_2}$）部分．

① 参閱第七章 §1 的 1．

这样看来,研究如何用尺規 n 等分圓周的問題,只需研究 n 是質数(大于 2) 的情形.

数学家高斯(Gauss)曾給出了下面的定理:

"可以利用圓規和直尺把圓周分割成 n 个等分的充分而且必要条件是: $n=2^k n_1 n_2 \cdots\cdots n_s$. 这里 k 为非負整数, n_1、n_2、……、n_s 为相异的奇質数,且每一个都有形式: 2^p+1."

大概由于費尔馬(Fermat)最先研究形如 2^p+1 的数,我們就把形如 2^p+1 的質数叫做費尔馬質数.

容易知道,求得費尔馬質数的必要条件是: p 是 2 的 n 次冪. 事实上,如果 p 还有不是 2 的質約数(显然,不是 2 的質約数必为奇数) m, 設 $p=mn$, 于是 $2^p+1=(2^n)^m+1$

$$=(2^n+1)[2^{n(m-1)}-2^{n(m-2)}+\cdots\cdots+1].$$

显然,这时 2^p+1 就不是質数了.

这样,我們就有理由假定 $p=2^n$.

設 $F_n=2^{2^n}+1$, 当 $n=0$、1、2、3、4 的时候, $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ 都是質数.根据这个事实,費尔馬曾猜測 F_n 一定是質数.但欧拉(Euler)于 1732 年举出:

$$F_5=4294967297=641\cdot 6700417.$$

就是說 F_5 是合数. 所以費尔馬的猜測并不眞实.

此外,陆續地由数学家們証明,当 $n=6$、7、8、9、11、12、18、23、36、38、73 的时候, F_n 都不是質数.

直到今天,除了 F_0、F_1、F_2、F_3、F_4 五个質数外,还沒有找到一个其他的費尔馬質数.

下面介紹有名的古特巴黑問題.

彼得堡科学院院士古特巴黑曾提到一个如下的問題:

"凡大于 2 的偶数,一定是两个質数的和; 凡大于 5 的奇数一定是三个質数的和."

他自己不能証明这个断言, 連当时已声譽很高的欧拉(他的朋友)

也不能証明它.这已經是两百多年以前的事了.

德国数学家藍陶在1912年国际数学会議上，曾說：古特巴黑問題是当代数学界所无法解决的，甚至解决下面的問題也会感到异常困难："存在一正整数C，而任一正整数N一定可表成不超过C个質数的和."

1930年，苏联杰出的数学家西涅莱尔曼（Шнирельман）解决了藍陶的問題，証明了："凡充分大的正整数一定是有限个質数的和."而且經过数学家們的努力，質数的个数逐渐改进到67，后来又改进到20.

对于古特巴黑問題有着划时代貢献的，当推苏联著名数学家維諾格拉多夫（Виноградов）院士．他在1937年証明了："凡充分大的奇数，都可表成三个質数的和."即証明了古特巴黑的断言在某奇数充分大的时候是成立的.

那末"充分大"究竟有多大？1939年苏联青年数学家波罗兹特金（Бороздкин）算出了这个界限为：

$$N_0=e^{e^{e^{41.96}}}$$

e是自然对数底.

留下来就是要大大的改进这个界限数.

我国数学家华罗庚教授在这个問題上也有卓越的貢献.他曾証明："几乎全部"偶数都是两質数的和.

屬于古特巴黑問題一类的有孿生質数問題.例如：3、5；5、7；11、13；17、19；29、31；41、43；71、73；……；10016957、10016959；等等.目前所知的一对最大的孿生質数是1000000009649、1000000009651.

問題就是是否存在无穷个相差为2的質数对，也即方程$p_1-p_2=2$是否有着无穷組質数解.

下面我們再談質数在自然数列中的分布規律問題.

尽管我們知道質数的个数是无限的，可是无法找到一个公式，按着它可以把一切質数写出来（假如有这种公式，我們对于龐大的質数表当

然就会失去兴趣).甚至只要找到一个公式能给出无限个质数(縱使不是全部的),也是办不到.

这样我們就有兴趣注意下面的一些公式:

公式 x^2-x+17,

当 $x=0$、1、2、……、16 的时候,給出了质数.

(例如, $x=17$, 那末 $17^2-17+17=17^2$ 就不是质数了.)

公式 x^2-x+41,

当 $x=0$、1、2、……、40 的时候,給出了质数.

又如,公式

$$x^2-x+19421,$$
$$x^2-x+27941,$$
$$x^2-x+72491$$

都代表着丰富的质数(譬如,最后的公式, 当 $x=0$、1、2、……、11000 的时候,給出了质数).

上面的内容,已专門形成一个問題:

"对于任意給定的正整数 N, 是否有整数 A 存在,使下式

$$x^2-x+A,$$

当 $x=0$、1、2、……、N 的时候,都表示质数."

这也是个沒有解决的問題.

至于质数在自然数列中的分布規律是极其复杂的.

設 $\pi(x)$ 表示一切不大于实数 x 的质数的个数. 例如,不大于 20.5 的质数共有 8 个,所以表示 $\pi(20.5)=8$.

我們从自然数中质数个数是无限多的这一点,就知道:如果

$$x\longrightarrow\infty, \quad 那末\ \pi(x)\longrightarrow\infty.$$

法国数学家勒讓得尔(Legendre)完善的証明了:"当 $x\longrightarrow\infty$ 时, $\frac{\pi(x)}{x}\longrightarrow0$." 就是說,质数在自然数列中的"密度"无限遞降.

人們自然地会想到去找寻公式,由 x 而求出 $\pi(x)$. 經过数学家們的努力工作,得到了近似公式.

勒讓得尔研究质数表时，得到結論："$\pi(x)$与$\frac{x}{\ln x}$差别很小（$\ln x$是x的自然对数）."数学家高斯也有过同样的結論.

对上面的断言，在偉大的俄国数学家切貝舍夫（Чебышев）院士之前，沒有一个数学家严格地証实过它. 1851年切貝舍夫証明了：

"存在两个常数c_1、c_2（c_1、c_2都大于0）、使

$$c_1\cdot\frac{x}{\ln x}<\pi(x)<c_2\cdot\frac{x}{\ln x}.$$

以后的一些数学家繼承了切貝舍夫的工作，更得到了如下的极限式：

$$\pi(x)=\lim_{x\to\infty}\frac{x}{\ln x}.$$

能更准确地表示$\pi(x)$的公式也早已求得，因为公式本身就带上积分記号，这里就不作介紹了.

順便也提一提被切貝舍夫証明了的"貝尔特朗（Bertrand）的推測."所謂貝尔特朗的推測，原来就是这样的一个論断：

"如果$n>1$，那末在n与$2n$之間，至少存在一个质数."

关于这个看来是显然的論断的証明，这里还沒有条件作介紹.

在质数理論中，所謂一些有趣問題，就零碎的介紹到这里.早就說过，这些所謂有趣問題，看来是如此的淺显，然而解决它們却会遇到簡直很难置信的困难.

第四章　若干数的最大公約数及最小公倍数的求法

有了前面几章的知識，才使我們可以严格地討論如何的求几个数的最大公約数和最小公倍数的問題.因为，首先我們有了求法的理論根据——最大公約数和最小公倍数的性质；其次，也有了具体計算的工

具——整除性判别法以及数的分解.

在本章中,我們将会看到求最大公約数和最小公倍数的各种方法,以及解决某些問题的特殊方法.

§1 利用数的分解求两数的最大公約数

定理 对于正整数 A、B,可設①

$$A=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n},\quad B=p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n}.$$

这里 p_1、p_2、……、p_n 是相异質数,α_i、β_i 是非負整数.又設 $\mathrm{Min}[\alpha_i,\ \beta_i]=\gamma_i$(就是 γ_i 是 α_i、β_i 中較小的一个).那末

$$(A,\ B)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots\cdots p_n^{\gamma_n}.$$

証明 因为 $\dfrac{p_i^{\alpha_i}}{p_i^{\gamma_i}}$ 和 $\dfrac{p_i^{\beta_i}}{p_i^{\gamma_i}}$ 中至少有一个等于1,也就是說,

$\left(\dfrac{p_i^{\alpha_i}}{p_i^{\gamma_i}},\ \dfrac{p_i^{\beta_i}}{p_i^{\gamma_i}}\right)=1$. 于是得到如下的 n 个等式:

$$\left(\frac{p_1^{\alpha_1}}{p_1^{\gamma_1}},\ \frac{p_1^{\beta_1}}{p_1^{\gamma_1}}\right)=1;$$

$$\left(\frac{p_2^{\alpha_2}}{p_2^{\gamma_2}},\ \frac{p_2^{\beta_2}}{p_2^{\gamma_2}}\right)=1;$$

$$\cdots\cdots\cdots\cdots;$$

$$\left(\frac{p_n^{\alpha_n}}{p_n^{\gamma_n}},\ \frac{p_n^{\beta_n}}{p_n^{\gamma_n}}\right)=1.$$

利用互質数的性質得

$$\left(\frac{p_1^{\alpha_1}}{p_1^{\gamma_1}}\cdots\cdots\frac{p_n^{\alpha_n}}{p_n^{\gamma_n}},\ \frac{p_1^{\beta_1}}{p_1^{\gamma_1}}\cdots\cdots\frac{p_n^{\beta_n}}{p_n^{\gamma_n}}\right)$$

$$=\left(\frac{A}{p_1^{\gamma_1}\cdots\cdots p_n^{\gamma_n}},\ \frac{B}{p_1^{\gamma_1}\cdots\cdots p_n^{\gamma_n}}\right)=1.$$

由第一章§2性質6就証明了:

---

① 譬如,对于 $51425=5^2\cdot 11^2\cdot 17$,$13310=2\cdot 5\cdot 11^3$,可看出:$51425=2^0\cdot 5^2\cdot 11^2\cdot 17$,$13310=2\cdot 5\cdot 11^3\cdot 17^0$.

$$(A, B)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots\cdots p_n^{\gamma_n}.$$

例1 求 $(24, 36)$.

$\because \quad 24=2^3\cdot 3, \quad 36=2^2\cdot 3^2,$

$\therefore \quad (24, 36)=2^2\cdot 3=12.$

例2 求 $(51425, 13310)$.

$\because \quad 51425=5^2\cdot 11^2\cdot 17, \quad 13310=2\cdot 5\cdot 11^3,$

$\therefore \quad (51425, 13310)=5\cdot 11^2=605.$

应用数的分解求两数的最大公約数是根据下面的定理:

$$\begin{array}{l|ll} p_1 & A & B \\ \hline p_2 & A_1 & B_1 \\ \hline & A_2 & B_2 \\ \hline & \cdots\cdots & \cdots\cdots \\ p_n & A_{n-1} & B_{n-1} \\ \hline & A_n & B_n \end{array}$$

設 A、B 是两个自然数(設它們不互質,不然最大公約数就是1).

設值大于1的 p_1 是 A、B 的公約数,而 A_1、B_1 分别为 p_1 除 A、B 所得的商.

如果 A_1、B_1 两数不互質,設 p_2 $(p_2\neq 1)$ 为 A_1、B_1 的公約数,而 A_2、B_2 分别为 p_2 除 A_1、B_1 所得的商. 下面就这样地繼續下去.

很清楚,这种过程不会是无限的,也就是說,一定能找到一个数 p_n,分别除 A_{n-1}、B_{n-1} 所得的商 A_n、B_n 是两个互質的数.那末,

$$(A, B)=p_1p_2\cdots\cdots p_n.$$

証明 因为 $A=p_1A_1=p_1(p_2A_2)=\cdots\cdots=(p_1p_2\cdots\cdots p_n)A_n$; 同理,$B=(p_1p_2\cdots\cdots p_n)B_n$.

已知 $(A_n, B_n)=1$,于是根据第一章§2性质6得

$$(A, B)=p_1p_2\cdots\cdots p_n.$$

[定理的証明也可这样进行:

因为 $(A, B)=(p_1p_2\cdots\cdots p_nA_n, \; p_1p_2\cdots\cdots p_nB_n)$

$$=p_1p_2\cdots\cdots p_n(A_n,\ B_n),$$

而已知$(A_n,\ B_n)=1$，所以$(A,\ B)=p_1p_2\cdots\cdots p_n$.]

从証明的过程中可知，p_1、p_2、……、p_n各数不一定限制为质数（也不一定按照由小到大的次序），因此这个求两数的最大公約数的方法，比前面講的方法要来得方便.

例1 求 (384, 480).

4	384	480
4	96	120
6	24	30
	4	5

已知 (4, 5)=1,

所以 (384, 480)=4·4·6=96.

例2 求 (353430, 530145).

可以根据整除性判别法来作如下的运算：

9	353430	530145
15	39270	58905
17	2618	3927
7	154	231
11	22	33
	2	3

显然，(2, 3)=1，所以得

$$(353430,\ 530145)=9\cdot15\cdot17\cdot7\cdot11=176715.$$

下面介紹特殊問題的特殊解法.

1. 利用定理：$(ma,\ mb)=m(a,\ b)$. 对于某些問題的解法在書写上可以与上述的有所不同.

例 求 (4800, 3600).

因为 (4800, 3600)=100(48, 36)，而(48, 36)=12,

所以 (4800, 3600)=100·12=1200.

2. 利用定理：如果$(a, b)=1$，那末$(ca, b)=(c, b)$. 对于某些問題的解法可以簡化如下.

例1 求 $(40, 12)$.

因为 $(40, 12)=(40, 3\cdot 4)$，而 $(40, 3)=1$，

所以 $(40, 12)=(40, 4)=4$.

例2 求 $(100, 35)$.

因为 $(100, 35)=(100, 7\cdot 5)$，而 $(100, 7)=1$，

所以 $(100, 35)=(100, 5)=5$.

例3 求$(50, 84)$.

$$(50, 84)=(50, 7\cdot 12)=(50, 12)$$
$$=(5\cdot 10, 12)=(10, 12)=2.$$

3. 利用定理：$(a^n, b^n)=(a,b)^n$，也可解决一些特殊問題.

例1 求 $(8^4, 10^4)$.

已知 $(8, 10)=2$，所以$(8^4, 10^4)=2^4=16$.

例2 求 $(729, 1728)$.

因为$729=9^3$，而$1728=12^3$，所以

$$(729, 1728)=(9^3, 12^3)=(9, 12)^3=3^3=27.$$

§2 利用欧几里德除法(輾轉相除法)求两数的最大公約数

复习第一章§2性质3欧几里德除法. 这样，我們就是用語言也会叙述如何求两数的最大公約数了.

求两数的最大公約数，可先以两数中的小数除大数，然后以所得的余数(若不为零)去除小数. 如果得到的第二个余数还不为零，再以第二个余数去除第一个余数. 这样繼續輾轉相除，直到余数为零而止. 在最后相除时所用的除数(也就是最后一个不为零的余数)就是所求的两个数的最大公約数.

这个方法，通常我們以下面的形式表达出来：

	a	b	q_1
	bq_1	r_1q_2	
q_2	r_1	r_2	q_3
	r_2q_3	r_3q_4	
q_4	r_3	r_4	
	…………	…………	
	r_{n-3}	r_{n-2}	q_{n-1}
	$r_{n-2}q_{n-1}$	$r_{n-1}q_n$	
q_n	r_{n-1}	$r_n=0$	

上面的形式实际上就表示了下面的 n 个等式：

$$a=bq_1+r_1 \quad (0<r_1<b);$$

$$b=r_1q_2+r_2 \quad (0<r_2<r_1);$$

$$r_1=r_2q_3+r_3 \quad (0<r_3<r_2);$$

$$\cdots\cdots\cdots\cdots\cdots\cdots;$$

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1} \quad (0<r_{n-1}<r_{n-2});$$

$$r_{n-2}=r_{n-1}q_n+r_n \quad (r_n=0).$$

这样，上面的那个形式的意义就很明显了.

例 1 求 (111, 118).

1	111	118	
	105	111	
1	6	7	15
	6	6	
	0	1	6

由左边运算可知：

(111, 118)=1.

例 2 求 (2809, 6731).

2	2809	6731	
	2226	5618	
1	583	1113	2
	530	583	
10	53	530	1
		530	
		0	

由左边运算可知：

(2809, 6731)=53.

我国古代数学家秦九韶发明的求两数的最大公約数的方法（它的理論根据与輾轉相除法的根据是一致的）：

“以大减小，更相减損，以求等数.”

这就是說，从两个数中的大数减去小数，直到得到的差比較小的数还小，再从小数减去所得的差.如此更相减損，直到得到相等的差数为止.最后所得的差数，就是这两个数的最大公約数.

例 1 求 $(72, 108)$.

72	108	
	72	
72	36	（108 减了一次 72 而得）
36		
36	36	

既然最后得到了相等的差数，所以

$$(72, 108)=36.$$

例 2 求 $(693, 819)$.

	693	819
		693
	693	126
	126	
（693 連减了五次 126 而得）	63	126
		63
	63	63

由上可知：$(693, 819)=63$.

如果我們理解了輾轉相除法的理論根据，有时还可以灵活地加以应用.

例 1 求 $(399, 380)$.

因为 $399-380=19$，所以 $(399, 380)=(19, 380)$. 而 $380 \vdots 19$. 因此 $(399, 380)=19$.

例 2 求 $(315, 357)$.

因为$(315, 357)=(315, 42)$,又 $315-42\cdot7=21$, 所以$(315, 357)=(21, 42)=21$.

例 3 求 $(1578, 787)$.

因为 $1578-787=791$, 所以$(1578, 787)=(791,787)=(4, 787)$. 容易断定$(4, 787)=1$.〔虽然通过計算立刻可以証实上面的断言是正确的, 不过我們也应該常常施展观察力: 787 显然不能被 4 整除,而且它被 4 除后余数也不会是 2 .也就是說,余数不是 1 就是 3 .这样, $(4, 787)$不是等于$(4, 1)$ 就是等于$(4, 3)$了. 也就是說$(4, 787)=1$.〕因此, $(1578, 787)=1$.

§3 求两个以上数的最大公約数

先用数的分解来解决这个間題.

定理 对于正整数 A、B、……、L,

可設

$$A=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n},$$

$$B=p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$L=p_1^{\mu_1}p_2^{\mu_2}\cdots\cdots p_n^{\mu_n},$$

又設

$$\mathrm{Min}\,[\alpha_i,\ \beta_i,\ \cdots\cdots,\ \mu_i]=t_i,$$

那末

$$(A,\ B,\ \cdots\cdots,\ L)=p_1^{t_1}\,p_2^{t_2}\cdots\cdots\ p_n^{t_n}.$$

根据第一章 §2 性質 10,只要証明:

$$\frac{A}{p_1^{t_1}\cdots\cdots p_n^{t_n}},\ \frac{B}{p_1^{t_1}\cdots\cdots p_n^{t_n}},\ \cdots\cdots,\ \frac{L}{p_1^{t_1}\cdots\cdots p_n^{t_n}}\text{等}$$

的最大公約数是 1 就够了.或者直接根据最大公約数的定义来証明.証明留給讀者.

例 求 $(48, 84, 120, 1296)$.

因为

$$48=2^4\cdot3,$$

$$84=2^2\cdot3\cdot7,$$

$$120=2^3\cdot3\cdot5,$$

$$1296=2^4\cdot3^4,$$

所以 $$(48,\ 84,\ 120,\ 1296)=2^2\cdot3=12.$$

利用数的分解求多个数的最大公約数，也可以应用如下的定理：

$$\begin{array}{r|llll}
p_1 & A & B & \cdots\cdots & L \\ \hline
p_2 & A_1 & B_1 & \cdots\cdots & L_1 \\ \hline
 & A_2 & B_2 & \cdots\cdots & L_2 \\
 & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\
p_n & A_{n-1} & B_{n-1} & \cdots\cdots & L_{n-1} \\ \hline
 & A_n & B_n & \cdots\cdots & L_n
\end{array}$$

設 A、B、……、L 这些数不互質，而 p_1 ($p_1\neq1$) 是这些数的一个公約数，設 A_1、B_1、……、L_1 分别为 p_1 除 A、B、……、L 所得的商。如果 A_1、B_1、……、L_1 不互質，設 p_2 ($p_2\neq1$) 是这些数的一个公約数，又設 A_2、B_2、……、L_2 分别为 p_2 除 A_1、B_1、……、L_1 所得的商。这样繼續下去，如果 A_n、B_n、……、L_n 为互質的数，那末

$$(A,\ B,\ \cdots\cdots,\ L)=p_1p_2\cdots\cdots p_n.$$

它的証明，留給讀者．(可以根据第一章 § 2 性質 10)

例 求 (162, 216, 378, 108).

根据上面的定理，作如下的計算：

$$\begin{array}{r|rrrr}
2 & 162 & 216 & 378 & 108 \\ \hline
3 & 81 & 108 & 189 & 54 \\ \hline
9 & 27 & 36 & 63 & 18 \\ \hline
 & 3 & 4 & 7 & 2
\end{array}$$

$$\because\ (3,4,7,2)=1,$$

$$\therefore\ (162,216,378,108)=2\cdot3\cdot9=54.$$

根据第一章 § 2 性質 7，也可以得到求多个数的最大公約数的法則．

例 1 求 (140, 245, 315).

1	140	245	
	105	140	
3	35	105	1
		105	
		0	

由左边可知 (140, 245)=35，
所以 (140, 245, 315)=(35, 315).
因为 315⋮35，即 (35, 315)=35，
因此 (140, 245, 315)=35.

例 2 求 (48, 72, 21, 15).

因为 (48, 72)=24，而 (24, 21)=3，

又 (3, 15)=3，所以 (48, 72, 21, 15)=3.

当然，也可以这样做：

因为 (48, 72)=24，而 (21, 15)=3，

所以 (48, 72, 21, 15)=(24, 3)=3.

已經知道，求多个数的最大公約数，可以从求其中任意两个数的最大公約数开始．而求两个数的最大公約数問題根据秦九韶的更相减损法[就是，如果 $a-b=c$，那末 $(a, b)=(b, c)$]，可以轉化为求两个較簡单的数的最大公約数問題．于是对于求多个数的最大公約数問題，当然也可以化做求較簡单的几个数的最大公約数問題．

譬如，求 (A, B, C)，而其中 $A>C$．

我們設 $A-C=D$，这样就得到

$$(A, B, C)=(D, B, C).$$

例 1 求 (752, 423, 329, 235).

因为 752−423=329，所以

(752, 423, 329, 235)=(329, 423, 329, 235)=(423, 329, 235).

又 423−329=94，所以 (423, 329, 235)=(94, 329, 235).

又 329−235=94，所以

(94, 329, 235)=(94, 94, 235)=(94, 235).

又 235−94·2=47，所以 (94, 235)=(94, 47)=47.

因此，(752, 423, 329, 235)=47.

例2 求 $(162, 216, 378, 108)$.

因为 $378-216=162$,所以

$(162, 216, 378, 108)=(162, 216, 162, 108)=(216, 162, 108)$.

又 $216-162=54$, 所以$(216, 162, 108)=(54, 162, 108)$.

又 $162 \vdots 54$, 又 $108 \vdots 54$, 所以$(54, 162, 108)=(54, 108)=54$.

例3 求 $(140, 245, 315)$.

因为 $315-245=70$,所以

$$(140, 245, 315)=(140, 245, 70)=(245, 70).$$

又 $245-70\cdot3=35$,所以$(245, 70)=(35, 70)=35$.

因此, $(140, 245, 315)=35$.

例4 求 $(823, 547, 443)$.

因为 $823-547=276$,所以 $(823, 547, 443)=(276, 547, 443)$.

又 $547-443=104$, 所以 $(276, 547, 443)=(276, 104, 443)$.

又 $443-104\cdot4=27$,所以 $(276, 104, 443)=(276, 104, 27)$.

又 $276-27\cdot10=6$, 所以 $(276, 104, 27)=(6, 104, 27)$.

又 $(6, 27)=3$, 所以 $(6, 104, 27)=(3, 104)=1$.

于是得: $(823, 547, 443)=1$.

最后,再研究几种特殊情形.

1. 求 n 个数的最大公約数,而这 n 个数中,有一些数(譬如有 r 个数)是另一些数(或仅是一个数)的倍数,那末求这 n 个数的最大公約数,就只需求剩下的 $n-r$ 个数的最大公約数.

例 求 $(24, 84, 21, 72, 7)$.

因为 $72 \vdots 24$, $84 \vdots 7$, $21 \vdots 7$,

所以 $(24, 84, 21, 72, 7)=(24, 7)$.

2. 如果发現 n 个数中有两个是互质的,那末这 n 个数的最大公約数一定是1.

例 求 $(90, 243, 5, 12)$.

可以发現: $(5, 12)=1$, 所以可断言 $(90, 243, 5, 12)=1$.

3. 如果发現 n 个数可以表示成指数相等的冪，那末可以利用定理：$(a_1^s, a_2^s, \cdots\cdots, a_n^s)=(a_1, a_2, \cdots\cdots, a_n)^s$ 来求这 n 个数的最大公約数.

例 求 $(64, 512, 216)$.

因为 $64=4^3$, $512=8^3$, $216=6^3$,

所以 $(64, 512, 216)=(4^3, 8^3, 6^3)=(4, 8, 6)^3=2^3=8$.

§4 求两个数的最小公倍数

根据第一章 §3 性质 5：$[a, b]=\dfrac{ab}{(a, b)}$，可以求两数的最小公倍数.

例 1 求 $[391, 493]$.

先求 $(391, 493)$.

1	391	493	
	306	391	
1	85	102	3
	85	85	
	0	17	5

就是說，$(391, 493)=17$，因此

$$[391, 493]=\frac{391\cdot 493}{17}=11339.$$

例 2 求 $[508, 889]$.

$\because$ $(508, 889)=(508, 381)=(127, 381)=(127, 127)=127$,

$\therefore$ $[508, 889]=\dfrac{508\cdot 889}{127}=3556$.

上述求两数最小公倍数的方法，必須先求出两数的最大公約数，所以方法不甚簡便. 我們也可以利用下面的定理.

定理 对于正整数 A、B，可設

$$A=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n},\quad B=p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n},$$

这里 p_1、p_2、……、p_n 是相异质数，α_i、β_i 是非负整数．且

$$\gamma_i=\text{Max}[\alpha_i,\ \beta_i]\quad（即\ \gamma_i\ 为\ \alpha_i\ 和\ \beta_i 中較大的一个）.$$

那末
$$[A,\ B]=p_1^{\gamma_1}p_2^{\gamma_2}\cdots\cdots p_n^{\gamma_n}.$$

証明 因为 $\dfrac{p_i^{\gamma_i}}{p_i^{\alpha_i}}$ 与 $\dfrac{p_i^{\gamma_i}}{p_i^{\beta_i}}$ 中一定有一个等于 1．

也就是
$$\left(\frac{p_i^{\gamma_i}}{p_i^{\alpha_i}},\ \frac{p_i^{\gamma_i}}{p_i^{\beta_i}}\right)=1.$$

于是就得到下面的一些等式：

$$\left(\frac{p_1^{\gamma_1}}{p_1^{\alpha_1}},\ \frac{p_1^{\gamma_1}}{p_1^{\beta_1}}\right)=1;$$

$$\left(\frac{p_2^{\gamma_2}}{p_2^{\alpha_2}},\ \frac{p_2^{\gamma_2}}{p_2^{\beta_2}}\right)=1;$$

$$\cdots\cdots\cdots\cdots;$$

$$\left(\frac{p_n^{\gamma_n}}{p_n^{\alpha_n}},\ \frac{p_n^{\gamma_n}}{p_n^{\beta_n}}\right)=1.$$

由互质数的性质可知：

$$\left(\frac{p_1^{\gamma_1}}{p_1^{\alpha_1}}\cdots\cdots\frac{p_n^{\gamma_n}}{p_n^{\alpha_n}},\ \frac{p_1^{\gamma_1}}{p_1^{\beta_1}}\cdots\cdots\frac{p_n^{\gamma_n}}{p_n^{\beta_n}}\right)=1.$$

也就是
$$\left(\frac{p_1^{\gamma_1}\cdots\cdots p_n^{\gamma_n}}{A},\ \frac{p_1^{\gamma_1}\cdots\cdots p_n^{\gamma_n}}{B}\right)=1.$$

由第一章 §3 性质 3 可知：

$$[A,\ B]=p_1^{\gamma_1}p_2^{\gamma_2}\cdots\cdots p_n^{\gamma_n}.$$

例 1 求 $[180,\ 300]$．

因为 $180=2^2\cdot3^2\cdot5$，而 $300=2^2\cdot3\cdot5^2$，

所以 $[180,\ 300]=2^2\cdot3^2\cdot5^2=900$．

例 2 求 $[720,\ 675]$．

因为 $720=2^4\cdot3^2\cdot5$，$675=3^3\cdot5^2$，

所以 $[720,\ 675]=2^4\cdot3^3\cdot5^2=10800$．

既然求两数的最小公倍数先把这两个数分解质因数，因此我們也可用下面的定理求两数的最小公倍数：

$$\begin{array}{r|ll} p_1 & A & B \\ \hline p_2 & A_1 & B_1 \\ \hline & A_2 & B_2 \\ & \cdots & \cdots\cdots \\ p_n & A_{n-1} & B_{n-1} \\ \hline & A_n & B_n \end{array}$$

設 A、B 是两正整数，且不互質. 設値大于 1 的 p_1 是 A、B 的公約数，而 A_1、B_1 分别是 p_1 除 A、B 所得的商.

这样繼續下去，显然最后能找到一数 p_n，用它除 A_{n-1}、B_{n-1} 所得的商 A_n、B_n 为互質的数. 如果这样，那末

$$[A, B]=p_1p_2\cdots\ p_n\cdot A_n\cdot B_n.$$

証明 已知 $A=p_1p_2\cdots\cdots p_nA_n$，$B=p_1p_2\cdots\cdots p_nB_n$，

所以 $[A, B]=[p_1p_2\cdots\cdots p_nA_n,\ p_1p_2\cdots\cdots p_nB_n]$

$=p_1p_2\cdots\cdots p_n[A_n,\ B_n]$.

因为 $(A_n, B_n)=1$，即有 $[A_n, B_n]=A_nB_n$，

所以 $[A, B]=p_1p_2\cdots\cdots p_nA_nB_n$.

例 1 求 $[720, 675]$.

$$\begin{array}{r|ll} 9 & 720 & 675 \\ \hline 5 & 80 & 75 \\ \hline & 16 & 15 \end{array}$$

因为 $(16, 15)=1$，所以 $[720, 675]=9\cdot5\cdot16\cdot15=10800$.

例 2 求 $[756, 504]$.

$$\begin{array}{r|ll} 9 & 756 & 504 \\ \hline 7 & 84 & 56 \\ \hline 4 & 12 & 8 \\ \hline & 3 & 2 \end{array}$$

因为 $(3, 2)=1$，所以 $[756, 504]=9\cdot7\cdot4\cdot3\cdot2=1512$.

下面研究几种特殊情形：

1. 利用定理："如果 $(a, c)=1$，那末$[a, bc]=c[a, b]$." 求两数的最小公倍数.

例 1 求 $[38, 42]$.

因为 $42=6\cdot7$，而 $(38, 7)=1$，所以

$$[38, 42]=7[38, 6].$$

又 $38=19\cdot2$，而 $(19, 6)=1$，于是

$$[38, 6]=19[2, 6]=19\cdot6.$$

所以 $[38, 42]=7\cdot[38, 6]=7\cdot19\cdot6=798$.

例 2 求 $[96, 132]$.

$$[96, 132]=4[24, 33]=4[24, 11\cdot3]$$
$$=4\cdot11[24, 3]=4\cdot11\cdot24=1056.$$

2. 利用定理："$[a^s, b^s]=[a, b]^s$." 求两数的最小公倍数.

例 求 $[64, 216]$.

因为 $64=4^3$，$216=6^3$，所以

$$[64, 216]=[4^3, 6^3]=[4, 6]^3=12^3.$$

§5 求两个以上数的最小公倍数

利用第一章 §3 性質 6 和它的推論，我們可以求多个数的最小公倍数.

例 1 求 $[15, 18, 20]$.

因为 $[15, 18]=3[5, 6]=3\cdot30=90$,

而 $[90, 20]=10[9, 2]=10\cdot18=180$,

所以 $[15, 18, 20]=180$.

例 2 求 $[16, 18, 20, 24]$.

因为 $[16, 18]=2[8, 9]=2\cdot72=144$,

而 $[144, 24]=144$. $(\because 144 \vdots 24)$

又$\because$ $[144, 20]=4[36, 5]=4\cdot36\cdot5=720$.

因此 $[16, 18, 20, 24]=720$.

当然也可以采用下面的方法：

因为 $[16, 18]=144$，而 $[20, 24]=4[5, 6]=120$,

所以 $[16, 18, 20, 24]=[144, 120]=24[6, 5]$

$$=24\cdot 30=720.$$

应用数的分解,也能求多个数的最小公倍数.

定理 对于正整数 A、B、……、L, 可設

$$A=p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_n^{\alpha_n},$$

$$B=p_1^{\beta_1}p_2^{\beta_2}\cdots\cdots p_n^{\beta_n},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$L=p_1^{\mu_1}p_2^{\mu_2}\cdots\cdots p_n^{\mu_n},$$

这里 p_1、p_2、……、p_n 是相异质数, 且 α_i、β_i、……、μ_i 是非負整数. 如果 $t_i=\text{Max}[\alpha_i, \beta_i, \cdots\cdots, \mu_i]$, 那末

$$[A、B、\cdots\cdots、L]=p_1^{t_1}p_2^{t_2}\cdots\cdots p_n^{t_n}.$$

根据第一章 §3 性质 8 这一定理可以获得証明;或直接按照最小公倍数的定义也可以.这里把証明留給讀者.

例 1 求 $[36, 48, 56]$.

因为 $36=2^2\cdot 3^2$, $48=2^4\cdot 3$, $56=2^3\cdot 7$,

所以 $[36, 48, 56]=2^4\cdot 3^2\cdot 7=1008$.

例 2 求 $[720, 675, 500, 450]$.

因为 $720=2^4\cdot 3^2\cdot 5$, $675=3^3\cdot 5^2$, $500=2^2\cdot 5^3$, $450=2\cdot 3^2\cdot 5^2$,

所以 $[720, 675, 500, 450]=2^4\cdot 3^3\cdot 5^3=54000$.

下面我們对求多个数的最小公倍数間題,再加以討論.

$$\begin{array}{r|cccc}
p_1 & A & B & \cdots\cdots & L \\ \hline
p_2 & A_1 & B_1 & \cdots\cdots & L_1 \\ \hline
 & A_2 & B_2 & \cdots\cdots & L_2 \\
 & \cdots & \cdots & \cdots\cdots & \cdots \\
p_n & A_{n-1} & B_{n-1} & \cdots\cdots & L_{n-1} \\ \hline
 & A_n & B_n & \cdots\cdots & L_n
\end{array}$$

我們已經熟悉了上面的形式. 如果最后得到的 A_n、B_n、……、L_n 等是互质的数,那末

$$[A, B, \cdots\cdots, L]=p_1p_2\cdots\cdots p_n[A_n, B_n, \cdots\cdots, L_n].$$

現在就需要解决 $[A_n, B_n, \cdots\cdots, L_n]$ 的大小問題.

当 $(A_n, B_n, \cdots\cdots, L_n)=1$ 的时候.

如果这时 A_n、B_n、……、L_n 等数两两互質，那末根据第一章§3 性質 6 的推論 3，可以知道 $[A_n, B_n, \cdots, L_n]=A_nB_n\cdots\cdots L_n$.

如果 A_n、B_n、……、L_n 并不两两互質，那末就需要利用第一章 §3 性質 10，就是：

"如果在 n 个数中，a_1、a_2、……、a_k 都能被 d 整除，而 a_{k+1}、a_{k+2}、……、a_n 都与 d 互質，那末

$$[a_1, a_2, \cdots\cdots, a_n]=d\left[\frac{a_1}{d}, \frac{a_2}{d}, \cdots\cdots, \frac{a_k}{d}, a_{k+1}, \cdots\cdots, a_n\right]."$$

例 1 求 $[15, 20, 24]$.

可以看到：$15 \vdots 5$，$20 \vdots 5$，而 $(24, 5)=1$，

所以 $[15, 20, 24]=5[3, 4, 24]$.

同样的，因为 $4 \vdots 4$，$24 \vdots 4$，而 $(3, 4)=1$，

所以 $[3, 4, 24]=4[3, 1, 6]=4\cdot6=24$.

也就是，$[15, 20, 24]=5\cdot24=120$.

例 2 求 $[28, 18, 20, 21, 24, 32]$.

可以看到：28, 18, 20, 24, 32 都能被 2 整除，而 $(21, 2)=1$，所以

$$[28, 18, 20, 21, 24, 32]=2[14, 9, 10, 21, 12, 16].$$

又 14, 10, 12, 16 都能被 2 整除，而 9, 21 都与 2 互質，所以

$$[14, 9, 10, 21, 12, 16]=2[7, 9, 5, 21, 6, 8].$$

又 6、9、21 都能被 3 整除，而 7、5、8 都与 3 互質，所以

$$[7, 9, 5, 21, 6, 8]=3[7, 3, 5, 7, 2, 8].$$

同理，$[7, 3, 5, 7, 2, 8]=7[1, 3, 5, 1, 2, 8]$.

同理，$[1, 3, 5, 1, 2, 8]=2[1, 3, 5, 1, 1, 4]$.

因为 3, 5, 4 两两互質，于是

$$[1, 3, 5, 1, 1, 4]=3\cdot5\cdot4.$$

綜合上述，得

$$[28, 18, 20, 21, 24, 32]=2\cdot2\cdot3\cdot7\cdot2\cdot3\cdot5\cdot4=10080.$$

为了書写方便起見，上面一系列的計算，可以安排如下：

$$\begin{array}{r|cccccc}
2 & 28 & 18 & 20 & 21 & 24 & 32 \\ \hline
2 & 14 & 9 & 10 & 21 & 12 & 16 \\ \hline
3 & 7 & 9 & 5 & 21 & 6 & 8 \\ \hline
7 & 7 & 3 & 5 & 7 & 2 & 8 \\ \hline
2 & 1 & 3 & 5 & 1 & 2 & 8 \\ \hline
 & 1 & 3 & 5 & 1 & 1 & 4
\end{array}$$

所以 $[28, 18, 20, 21, 24, 32]=2\cdot2\cdot3\cdot7\cdot2\cdot3\cdot5\cdot4=10080.$

例3 求$[15, 18, 20]$.

$$\begin{array}{r|ccc}
3 & 15 & 18 & 20 \\ \hline
5 & 5 & 6 & 20 \\ \hline
2 & 1 & 6 & 4 \\ \hline
 & 1 & 3 & 2
\end{array}$$

由上可知：$[15, 18, 20]=3\cdot5\cdot2\cdot3\cdot2=180.$

例4 求 $[18, 24, 27, 45]$.

$$\begin{array}{r|cccc}
3 & 18 & 24 & 27 & 45 \\ \hline
3 & 6 & 8 & 9 & 15 \\ \hline
2 & 2 & 8 & 3 & 5 \\ \hline
 & 1 & 4 & 3 & 5
\end{array}$$

因为 4, 3, 5 两两互質，所以

$$[18, 24, 27, 45]=3\cdot3\cdot2\cdot4\cdot3\cdot5=1080.$$

最后，再研究几种特殊情况.

1. 如果n个数中，有k个数是某一些(或仅是一个数)的約数，那末求这n个数的最小公倍数，就只需求剩下的$n-k$个数的最小公倍数.

例1 求 $[15, 24, 40, 80, 60]$.

这里　60⋮15, 80⋮40,所以

$$[15,24,40,80,60]=[24,80,60]$$
$$=4[6,20,15]=4\cdot3[2,20,5].$$

而　2, 5都是20的約数,就是 $[2,20,5]=20$.

所以　$[15,24,40,80,60]=4\cdot3\cdot20=240$.

例2　求 $[15,20,36,40,84]$.

```
4 | 15  20  36  40  84 (这里20是40的約数)
  -------------------------
3 | 15       9  10  21
  -------------------------
     5       3  10   7 (这里 5 是10的約数)
```

因为　3, 10, 7两两互质,所以

$$[15,20,36,40,84]=4\cdot3\cdot3\cdot10\cdot7=2520.$$

例3　求 $[16,48,32,96,12]$.

因为96是其他四个数的倍数,所以結果是96.

2. 利用定理: $[a_1^s, a_2^s, \cdots\cdots, a_n^s]=[a_1, a_2, \cdots\cdots, a_n]^s$. 可以求多个数的最小公倍数.

例　求 $[64,512,216]$.

因为 $64=4^3$, $512=8^3$, $216=6^3$,

所以 $[64,512,216]=[4^3,8^3,6^3]$

$$=[4,8,6]^3=24^3=13824.$$

到这里为止，我們詳細的探討了求两个数和几个数的最大公約数和最小公倍数的間題,同时也討論了若干計算的技巧間題.这里我們也就結束了有关整除性理論的探討.

下一章我們將探究关于“剩余”間題，它是一个内容十分丰富而有趣的間題.它也是数論的一个基础．因限于这个册子的性质,关于这个間題当然我們无法談的很多.

第五章　剩　余

在整数的理論中，"同余"这个問題的研究占了很大的比重。这也就說明了它的重要性。可以說，同余这个概念的引入，在不小的程度上丰富了数学的內容。关于这一点，尽管这个册子不是专門研究同余理論的，但是我們还是可以从本章中看到的。

§1　同余的基本概念

对于整数 a、b 及正整数 m 有下列关系：

$$a = mq_1 + r_1, \quad (0 \leqslant r_1 < m)$$

$$b = mq_2 + r_2, \quad (0 \leqslant r_2 < m)$$

而 $$r_1 = r_2;$$

那末，我們說 a、b 对于模数 m 为同余(也可以說：对于模数 m，a、b 同余)。記作：

$$a \equiv b \pmod{m}.$$

上式叫做同余式。

譬如，42、50 被 8 除，得到的余数都是 2，于是說：40、50 对于模数 8 为同余。記作：　$42 \equiv 50 \pmod{8}$.

又如，-11、16 被 3 除，得到的余数都是 1，也就是說，

$$-11 \equiv 16 \pmod{3}.$$

定理　a、b 对于模数 m 同余的充分而且必要条件是：

$$a - b \vdots m.$$

証明　1. 条件的充分性：

設 $a = mq_1 + r_1$ $(0 \leqslant r_1 < m)$，$b = mq_2 + r_2$ $(0 \leqslant r_2 < m)$。于是 $a - b = m(q_1 - q_2) + (r_1 - r_2)$.

因为 $a - b \vdots m$，于是 $r_1 - r_2 \vdots m$。而只有当 $r_1 = r_2$ 的时候，$r_1 - r_2 \vdots m$。所以 $a \equiv b \pmod{m}$.

2. 条件的必要性.

如果 $a\equiv b \pmod{m}$，那末

$$a=mq_1+r,\quad b=mq_2+r.$$

很明显，
$$a-b=m(q_1-q_2)\ \vdots\ m.$$

推論 1 $$a\equiv a \pmod{m}.$$

推論 2 $$a\equiv b \pmod{m}$$

与 $b\equiv a \pmod{m}$ 等价.

推論 3 $$a\equiv b \pmod{m}$$

与 $a-b\equiv 0 \pmod{m}$ 等价.

上面三个推論的論証，留給讀者.

推論 4 如果 $a\equiv b \pmod{m}$，$b\equiv c \pmod{m}$，那末

$$a\equiv c \pmod{m}.$$

証明 因为 $a-b\ \vdots\ m$，$b-c\ \vdots\ m$，所以

$$(a-b)+(b-c)=a-c\ \vdots\ m.$$

也就是說，
$$a\equiv c \pmod{m}.$$

推論 5 如果 $a\equiv b \pmod{m}$，m_1 是 m 的約数，那末

$$a\equiv b \pmod{m_1}.$$

証明 由 $a\equiv b \pmod{m}$ 得 $a-b\ \vdots\ m$.

因为 $m\ \vdots\ m_1$，所以 $a-b\ \vdots\ m_1$. 这样就推得：

$$a\equiv b \pmod{m_1}.$$

§2 同余的基本性質

1. 如果 $a\equiv b \pmod{m}$，$c\equiv d \pmod{m}$，

那末
$$a+c\equiv b+d \pmod{m}.$$

証明 由已知的条件可得：

$$a-b\ \vdots\ m,\quad c-d\ \vdots\ m.$$

显然，
$$(a-b)+(c-d)\ \vdots\ m,$$

也就是
$$(a+c)-(b+d)\ \vdots\ m.$$

由上节定理就得到：$a+c\equiv b+d \pmod{m}$.

这一定理显然可以推广到：多个数对同一模数同余的情形.

推論 1 如果 $a\equiv b \pmod{m}$，$c\equiv d \pmod{m}$，

那末 $$a-c\equiv b-d \pmod{m}.$$

証明 由 $c\equiv d \pmod{m}$，容易推得：$-c\equiv -d \pmod{m}$. 根据同余的性質就得到：

$$a-c\equiv b-d \pmod{m}.$$

推論 2 如果 $a\equiv b \pmod{m}$，而 c 是任一整数，那末

$$a+c\equiv b+c \pmod{m}.$$

証明 由 $a\equiv b \pmod{m}$ 及 $c\equiv c \pmod{m}$，根据同余的性質，就可以得到 $$a+c\equiv b+c \pmod{m}.$$

推論 3 同余式的两边可以移項.

如从 $a+b\equiv c \pmod{m}$，可以推出 $a\equiv c-b \pmod{m}$，等等.

推論 4 如果 $a\equiv b \pmod{m}$，那末

$$a\equiv b+mk \pmod{m}. \text{（}k\text{ 是任一整数）}$$

証明 由 $a\equiv b \pmod{m}$ 及 $0\equiv mk \pmod{m}$，就可以得到

$$a\equiv b+mk \pmod{m}.$$

2. 如果 $a\equiv b \pmod{m}$，$c\equiv d \pmod{m}$，那末

$$ac\equiv bd \pmod{m}.$$

証明 因为 $a-b \vdots m$，于是 $(a-b)c \vdots m$，也就是 $ac-bc \vdots m$. 因此 $ac\equiv bc \pmod{m}$.

因为 $c-d \vdots m$，于是 $(c-d)b \vdots m$，也就是 $bc-bd \vdots m$. 因此 $bc\equiv bd \pmod{m}$.

所以 $ac\equiv bd \pmod{m}$.（根据上节定理的推論 4）

这一定理显然可以推广到：多个数对同一模数的同余的情形.

推論 如果 $a\equiv b \pmod{m}$，那末

$$a^n\equiv b^n \pmod{m}. \text{（}n\text{ 为一非負整数）}$$

这就是性質 2 的特殊情形.

当 n 是正整数的时候，这个推論是成立的．事实上，当 $n=0$ 的时候，推論也成立．因为这时 $a^n\equiv b^n \pmod{m}$ 变成了 $1\equiv 1 \pmod{m}$．

例 1 求証：$a^m-b^m \vdots a-b$．

（这里 a、b 是不相等的两个整数，m 是正整数）．

証明 因为 $a\equiv b \pmod{a-b}$，所以 $a^m\equiv b^m \pmod{a-b}$．也就是說，$a^m-b^m \vdots a-b$．

当然很容易推得：

当 m 是偶数的时候，$a^m-b^m \vdots a+b$；

当 m 是奇数的时候，$a^m+b^m \vdots a+b$．

例 2 求 50^{13} 被 7 除所得的余数．

因为 $50\equiv 1 \pmod{7}$，所以 $50^{13}\equiv 1^{13} \pmod{7}$．

就是說，50^{13} 被 7 除，得到的余数是 1．

例 3 求 2^{40} 被 23 除所得的余数．

因为 $2^5=32$，所以 $2^5\equiv 9 \pmod{23}$．从而 $2^{10}\equiv 81 \pmod{23}$．又 $81\equiv 12 \pmod{23}$，所以得到 $2^{10}\equiv 12 \pmod{23}$．[我們可以把上面的意思写成：$2^{10}\equiv 81\equiv 12 \pmod{23}$．]

于是得到： $2^{20}\equiv 144\equiv 6 \pmod{23}$．

因此 $2^{40}\equiv 36\equiv 13 \pmod{23}$．

这就是說，2^{40} 被 23 除，得到的余数是 13．

例 4 求証：641 是 $2^{2^5}+1$ 的約数．

証明 因为 $2^{2^5}=2^{32}$，所以就需要証明：$2^{32}+1 \vdots 641$．

因为 $2^8=256$，所以 2^{16} $(2^{16}=65536)\equiv 154 \pmod{641}$．

从而 $2^{32}\equiv 154^2$ $(154^2=23716)\equiv -1 \pmod{641}$．

这就証明了 $2^{32}+1 \vdots 641$．

例 5 如果 $a^2\equiv 1 \pmod{m}$，那末

(1) 如果 p、q 同是奇数，$(m-a)^p+a^q \vdots m$；

(2) 如果 p、q 同是偶数，$(m-a)^p-a^q \vdots m$；

(3) 如果 p、q 同是奇数或同是偶数，$(m+a)^p-a^q \vdots m$．

証明(1) 因为 $a^2\equiv 1 \pmod m$，而 q 是奇数，設 $q=2t+1$（t 是非負整数），于是 $a^q=a^{2t+1}=a^{2t}\cdot a$.

而 $a^{2t}=(a^2)^t\equiv 1 \pmod m$，所以 $a^q\equiv a \pmod m$.

又因为 $(m-a)^2\equiv a^2\equiv 1 \pmod m$，而 p 也是奇数，同理，

$$(m-a)^p\equiv m-a \pmod m.$$

于是 $$(m-a)^p+a^q\equiv 0 \pmod m.$$

因此，$$(m-a)^p+a^q \vdots m.$$

(2) 因为 p、q 同是偶数，所以

$$a^q\equiv 1 \pmod m,\quad (m-a)^p\equiv 1 \pmod m.$$

于是 $$(m-a)^p-a^q\equiv 0 \pmod m,$$

因此，$$(m-a)^p-a^q \vdots m.$$

(3) 当 p、q 同为奇数的时候：

因为 $(m+a)^2\equiv a^2\equiv 1 \pmod m$，于是

$$a^q\equiv a \pmod m,\quad (m+a)^p\equiv m+a \pmod m.$$

所以 $$(m+a)^p-a^q\equiv 0 \pmod m.$$

也就是說，$$(m+a)^p-a^q \vdots m.$$

当 p、q 同是偶数的时候：

因为 $a^q\equiv 1 \pmod m$，$(m+a)^p\equiv 1 \pmod m$，

所以 $$(m+a)^p-a^q\equiv 0 \pmod m.$$

因此 $$(m+a)^p-a^q \vdots m.$$

[事实上，(3)就是(1)和(2)的推論.]

譬如，由 $11^2\equiv 1 \pmod{40}$，可断言：

$29^p+11^q \vdots 40$；（如果 p、q 同是奇数）

$29^p-11^q \vdots 40$；（如果 p、q 同是偶数）

$51^p-11^q \vdots 40$.（如果 p、q 同是奇数或同是偶数）

又如，由 $43^2\equiv 1 \pmod{66}$，可断言：

$23^p+43^q \vdots 66$；（如果 p、q 同是奇数）

$23^p-43^q \vdots 66$；（如果 p、q 同是偶数）

$$109^p-43^q:66.$$（如果 p、q 同是奇数或同是偶数）

由上面的两条基本性质，可推得：

如果 $\sum Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots\cdots x_n^{\alpha_n}$ 为一整系数整多项式，B、y_1、y_2、……、y_n 等数分别与 A、x_1、x_2、……、x_n 几个数对于模数 m 同余，那末

$$\sum Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots\cdots x_n^{\alpha_n}\equiv\sum By_1^{\alpha_1}y_2^{\alpha_2}\cdots\cdots y_n^{\alpha_n}\ (\mathrm{mod}\ m) \qquad (\mathrm{I})$$

証明 因为 $x_i\equiv y_i\ (\mathrm{mod}\ m)$，$i=1$、2、……、$n$.

当然 $x_i^{\alpha_i}\equiv y_i^{\alpha_i}\ (\mathrm{mod}\ m)$.

又知 $A\equiv B\ (\mathrm{mod}\ m)$.

所以 $Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots\cdots x_n^{\alpha_n}\equiv By_1^{\alpha_1}y_2^{\alpha_2}\cdots\cdots y_n^{\alpha_n}\ (\mathrm{mod}\ m)$.

显然，根据性质 1 就可以得到(I)．（$\sum Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots\cdots x_n^{\alpha_n}$ 是一切形如 $Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots\cdots x_n^{\alpha_n}$ 的单項式的和）

例如，多项式 $14x^5-25x^4+35x^3+15x^2-19x+5$ 对于模数 7 与 $3x^4+x^2+2x-2$ 同余．

这是因为：

$$14x^5\equiv 0\ (\mathrm{mod}\ 7);$$
$$-25x^4\equiv 3x^4\ (\mathrm{mod}\ 7);$$
$$35x^3\equiv 0\ (\mathrm{mod}\ 7);$$
$$15x^2\equiv x^2\ (\mathrm{mod}\ 7);$$
$$-19x\equiv 2x\ (\mathrm{mod}\ 7);$$
$$5\equiv -2\ (\mathrm{mod}\ 7).$$

因此上面的断言是成立的．

例 对于数 $\overline{a_na_{n-1}\cdots\cdots a_1a_0}$，如果

$10\equiv p_1\ (\mathrm{mod}\ m)$，$10^2\equiv p_2\ (\mathrm{mod}\ m)$，……，$10^n\equiv p_n\ (\mathrm{mod}\ m)$，

那末 $\overline{a_n\cdots\cdots a_1a_0}\equiv a_np_n+a_{n-1}p_{n-1}+\cdots\cdots+a_1p_1+a_0\ (\mathrm{mod}\ m)$.

証明留給讀者．

譬如，求 24657 被 23 除所得的余数．

因为 $10\equiv 10(\mathrm{mod}\ 23)$，$10^2\equiv 8(\mathrm{mod}\ 23)$，$10^3\equiv 80\equiv 11(\mathrm{mod}\ 23)$，$10^4\equiv 8^2\equiv 18(\mathrm{mod}\ 23)$［或 $10^4\equiv -5(\mathrm{mod}\ 23)$］，

所以 $24657\equiv 18\cdot 2+11\cdot 4+8\cdot 6+10\cdot 5+7\ (\mathrm{mod}\ 23)$.

而 $18\cdot 2=36\equiv 13 \pmod{23}$， $11\cdot 4\equiv 21 \pmod{23}$，

$8\cdot 6\equiv 2 \pmod{23}$， $10\cdot 5\equiv 4 \pmod{23}$.

又 $13+21+2+4+7\equiv 1 \pmod{23}$，所以 $24657\equiv 1 \pmod{23}$.

又如：求 85673 被 47 除所得的余数.

因为
$$10^2\equiv 6 \pmod{47},$$
$$10^3\equiv 60\equiv 13 \pmod{47},$$
$$10^4\equiv 6^2\equiv -11 \pmod{47},$$

所以 $85673\equiv(-11)\cdot 8+13\cdot 5+6\cdot 6+10\cdot 7+3\equiv 39 \pmod{47}$.

3．如果同余式 $a\equiv b \pmod{x}$ 对于 x 分别是 m_1、m_2、……、m_k 时都成立，設 $[m_1, m_2, \cdots\cdots, m_k]=M$，那末 $a\equiv b \pmod{M}$.

証明 因为 $a-b$ 能被 m_1、m_2、……、m_k 等数整除，所以 $a-b$ 一定能被这些数的最小公倍数 M 所整除．既然 $a-b \vdots M$，所以

$$a\equiv b \pmod{M}.$$

4．如果 $a\equiv b \pmod{m}$，d 是非零整数，而 $a \vdots |d|$， $b \vdots |d|$，且 $(|d|, m)=1$，那末
$$\frac{a}{d}\equiv\frac{b}{d} \pmod{m}.$$

証明 設 $a=dq_1$， $b=dq_2$．由条件可知 $a-b \vdots m$，也就是
$$d(q_1-q_2) \vdots m.$$

已知 $(|d|, m)=1$，所以 $q_1-q_2 \vdots m$．于是

$$q_1\equiv q_2 \pmod{m}. \text{ 也就是說，} \frac{a}{d}\equiv\frac{b}{d} \pmod{m}.$$

注意 从这条性质可以看到，同余式与等式在性质上并不都相类似的.

如由 $24\equiv 4 \pmod{10}$ 就不能推得 $\frac{24}{4}\equiv\frac{4}{4} \pmod{10}$． 这里 $(4, 10)>1$.

5．如果 $a\equiv b \pmod{m}$，那末 $ak\equiv bk \pmod{m|k|}$．（k 是非零整数）

証明 因为 $a-b \vdots m$，所以 $k(a-b) \vdots m|k|$.

于是　　　　$ak-bk \vdots m|k|$，

因此　　　　$ak \equiv bk \pmod{m|k|}$.

6. 如果 $a \equiv b \pmod{m}$，d 是非零整数，而 $a \vdots |d|$，$m \vdots |d|$；那末 $b \vdots |d|$，且 $\frac{a}{d} \equiv \frac{b}{d}\left(\bmod \frac{m}{|d|}\right)$.

証明　因为 $a-b \vdots m$，而已知 $m \vdots |d|$，所以 $a-b \vdots |d|$. 由于 $a \vdots |d|$，因此得 $b \vdots |d|$.

由 $a-b \vdots |d|$，$m \vdots |d|$，可以知道 $\frac{a-b}{d} \vdots \frac{m}{|d|}$. 也就是說，

$$\frac{a}{d}-\frac{b}{d} \vdots \frac{m}{|d|}. \text{ 所以 } \frac{a}{d} \equiv \frac{b}{d}\left(\bmod \frac{m}{|d|}\right).$$

§3　一数被另一数除后余数的求法

这里准备探討求一数被另一数除后的余数問題. 我們可以想起第二章 §1 的定理：

如果 $10^k-M \vdots D$，(k 是正整数，M 是任意整数)那末

(1) $N \vdots D \rightleftarrows A \vdots D$; $[A=A_{0(k)}+MA_{1(k)}+\cdots\cdots+M^tA_{t(k)}]$

(2) $N \vdots D \rightleftarrows A' \vdots D$. $[A'=\overline{a_n\cdots\cdots a_k}\cdot M+A_{0(k)}]$

(这里 $N=\overline{a_na_{n-1}\cdots\cdots a_1a_0}$)

这条定理可以用来求一数被另一数除后的余数，只要把它改写成：

如果 $10^k \equiv M \pmod{D}$，那末

(1) $N \equiv A \pmod{D}$; $[A=A_{0(k)}+MA_{1(k)}+\cdots\cdots+M^tA_{t(k)}]$

(2) $N \equiv A' \pmod{D}$. $[A'=\overline{a_n\cdots\cdots a_k}\cdot M+A_{0(k)}]$

(这里不需重新再作証明了. 事实上，在前面已給我們指出了 $N-A \vdots D$ 与 $N-A' \vdots D$. 讀者可以参閱第二章 §1 定理的証明.)

例如，如果 $10^k \vdots D$，那末

$$N \equiv A_{0(k)}=\overline{a_k\cdots\cdots a_1a_0} \pmod{D}.$$

例　因为 $10 \equiv 1 \pmod{9}$，所以

$$N \equiv A = A_{0(1)} + A_{1(1)} + \cdots\cdots + A_{t(1)}$$
$$= a_0 + a_1 + \cdots\cdots + a_n \pmod 9.$$

（显然，上式对于模数是 3 的时候也成立.）

例 $N \equiv A = 2^2 a_2 + 2a_1 + a_0 \pmod 8$.

如何推出，留給讀者思考.

例 因为 $10 \equiv 3 \pmod 7$，所以

$$N \equiv A = a_0 + 3a_1 + 3^2 a_2 + \cdots\cdots + 3^n a_n \pmod 7.$$

又 $10^3 \equiv -1 \pmod 7$，所以

$$N \equiv A = A_{0(3)} - A_{1(3)} + A_{2(3)} - \cdots\cdots + (-1)^t A_{t(3)} \pmod 7.$$

（上式对模数 11、13 也成立.）

例 当 $D=11$ 时，由上例可知已有了求余数的法则. 不过由于 $10 \equiv -1 \pmod{11}$，所以另有

$$N \equiv A = a_0 - a_1 + a_2 - \cdots\cdots + (-1)^n a_n \pmod{11}.$$

此外，因为 $10^2 \equiv 1 \pmod{11}$，所以

$$N \equiv A = A_{0(2)} + A_{1(2)} + \cdots\cdots + A_{t(2)} \pmod{11}.$$

（上式对模数 33、99 也成立.）

例 当 $D=13$ 时，由前一例可以知道已經有了求余数的法则. 但是，我們还可以得到

$$N \equiv A = a_0 - 3a_1 + 3^2 a_2 - \cdots\cdots + (-3)^n a_n \pmod{13}$$

以及

$$N \equiv A = A_{0(2)} - 4A_{1(2)} + 4^2 A_{2(2)} - \cdots\cdots + (-4)^t A_{t(2)} \pmod{13}$$

两个关系. 上面两式如何推出，留給讀者思考.

下面举若干如何求余数的具体例题.

例 1 求 324673 被 9 除后的余数.

$$324673 \equiv 3+7+6+4+2+3 \equiv 7 \pmod 9.$$

例 2 求 52732 被 8 除后的余数.

$$52732 \equiv 2^2 \cdot 7 + 2 \cdot 3 + 2 \equiv 4 \pmod 8.$$

例 3 求 7423415 被 11 除后的余数.

用下面几种方法来求：

(1) $7423415 \equiv 5-1+4-3+2-4+7 \equiv 10 \pmod{11}$;

(2) $7423415 \equiv 15+34+42+7 \equiv 10 \pmod{11}$;

(3) $7423415 \equiv 415-423+7 \equiv 10 \pmod{11}$.

例 4 求 345750213 被 7 除后的余数.

$$345750213 \equiv 213-750+345 = -192 \pmod{7}.$$

当然直接求 -192 被 7 除后的非负最小剩余也是不困难的，不过可以这样做：

因为 $192 \equiv 2+3\cdot 9+3^2 \equiv 3 \pmod{7}$,

于是 $-192 \equiv -3 \equiv 4 \pmod{7}$.

所以 $345750213 \equiv 4 \pmod{7}$.

例 5 求 85673 被 47 除后的余数.

因为 $10^2 \equiv 6 \pmod{47}$，所以

$$85673 \equiv 73+6\cdot 56+6^2\cdot 8 = 697 \pmod{47}.$$

又 $697 \equiv 97+6\cdot 6 = 133 \pmod{47}$,

而 $133 \equiv 33+6 = 39 \pmod{47}$.

因此 $85673 \equiv 39 \pmod{47}$.

例 6 求 292000 被 97 除后的余数.

因为 $10^2 \equiv 3 \pmod{97}$，所以

$$292000 \equiv 0+3\cdot 20+3^2\cdot 29 = 321 \pmod{97};$$

而 $321 \equiv 21+3\cdot 3 = 30 \pmod{97}$.

因此 $292000 \equiv 30 \pmod{97}$.

例 7 求 981758 被 101 除后的余数.

因为 $10^2 \equiv -1 \pmod{101}$，所以

$$981758 \equiv 58-17+98 \equiv 38 \pmod{101}.$$

例 8 求 14995121 被 499 除后的余数.

因为 $10^3 \equiv 2 \pmod{499}$，故

$$14995121 \equiv 121+2\cdot 995+2^2\cdot 14 = 2167 \pmod{499}.$$

而 $2167 \equiv 167 + 2 \cdot 2 = 171 \pmod{499}$.

因此 $14995121 \equiv 171 \pmod{499}$.

例 9 求 3360274 被 167 除后的余数.

因为 $10^3 \equiv -2 \pmod{167}$, 故

$$3360274 \equiv 274 - 2 \cdot 360 + 2^2 \cdot 3 \equiv 67 \pmod{167}.$$

例 10 求 51860427 被 503 除后的余数.

因为 $10^3 \equiv -6 \pmod{503}$, 所以

$$51860427 \equiv 427 - 6 \cdot 860 + 6^2 \cdot 51$$
$$\equiv -2897 \pmod{503}.$$

而 $2897 \equiv 897 - 6 \cdot 2 \equiv 382 \pmod{503}$.

于是 $-2897 \equiv -382 \equiv 121 \pmod{503}$.

因此 $51860427 \equiv 121 \pmod{503}$.

例 11 求 4039500 被 1999 除后的余数.

因为 $10^4 \equiv 5 \pmod{1999}$, 所以

$$4039500 \equiv 9500 + 5 \cdot 403$$
$$= 11515 \pmod{1999}.$$

而 $11515 \equiv 1515 + 5 = 1520 \pmod{1999}$.

因此 $4039500 \equiv 1520 \pmod{1999}$.

通过这些例子,我們已初步地掌握了这个定理的应用. 事实上,当D不大,而N也不很大的时候, 求N被D除后的余数問題, 也可依照上节 2 中最后的一个例題所示的內容来解决.

§4 弃九驗算法

1. 如果 $a+b=c$, 設 $a \equiv r_1 \pmod{9}$, $b \equiv r_2 \pmod{9}$, $c \equiv r_3 \pmod{9}$, 那末 $r_1 + r_2 \equiv r_3 \pmod{9}$.

証明 因为 $a \equiv r_1 \pmod{9}$, $b \equiv r_2 \pmod{9}$,

所以 $a + b \equiv r_1 + r_2 \pmod{9}$.

又 $c \equiv r_3 \pmod{9}$, 而 $a+b=c$, 因此得

$$r_1+r_2\equiv r_3 \pmod 9.$$

对于上面的 r_1、r_2、r_3，如果取的是非負最小剩余，那末

当 $r_1+r_2<9$ 的时候，$r_1+r_2=r_3$；

当 $r_1+r_2\geqslant 9$ 的时候，設 r'_3 是 r_1+r_2 被 9 除后的非負最小剩余，于是 $r'_3=r_3$.

例 加法 $3748+6239=9987$.

容易看到：$3748\equiv 3+7+4+8\equiv 4 \pmod 9)$；

$$6239\equiv 6+2+3+9\equiv 2 \pmod 9;$$

$$9987\equiv 9+9+8+7\equiv 6 \pmod 9.$$

很明显，4、2、6 三个数的关系是：$4+2=6$.

我們可以用这一定理来檢驗加法运算是否正确．把定理写成另一个与它等价的形式：

設 $a\equiv r_1 \pmod 9$，$b\equiv r_2 \pmod 9$，$c\equiv r_3 \pmod 9$，如果 r_1+r_2 与 r_3 对于模数 9 不同余，那末 $a+b\neq c$.

例 檢驗 $4568+7391=11859$ 是否正确.

很容易看到：
$$4568\equiv 5 \pmod 9;$$
$$7391\equiv 2 \pmod 9;$$
$$11859\equiv 6 \pmod 9.$$

因为 $5+2=7$，而与 6 对于模数 9 不同余，所以上述的加法运算不正确.

显然，上述定理可推广到多个数相加的情形.

对减法运算的檢驗，直接可由上面的定理推出：

如果 $a-b=c$，設 $a\equiv r_1 \pmod 9$，$b\equiv r_2 \pmod 9$，$c\equiv r_3 \pmod 9$，那末 $r_2+r_3\equiv r_1 \pmod 9$.

例 檢驗减法运算 $7391-4568=2823$ 是否正确.

很容易看到：
$$7391\equiv 2 \pmod 9;$$
$$4568\equiv 5 \pmod 9;$$
$$2823\equiv 6 \pmod 9.$$

显然，$6+5\equiv 2 \pmod 9$，所以

$$7391-4568=2823 \text{ 是正确的.}$$

注 在定理中，$r_1+r_2\equiv r_3 \pmod 9$ 仅是 $a+b=c$ 的必要条件，而不是充分条件．也就是說，有时 $r_1+r_2\equiv r_3 \pmod 9$ 虽成立，而 $a+b=c$ 却不一定成立．譬如：$4568+7391=11959$.

容易看到：

$4568\equiv 5 \pmod 9$，$7391\equiv 2 \pmod 9$，$11959\equiv 7 \pmod 9$.

显然，$5+2\equiv 7 \pmod 9$.

如果把 11959 誤写作 11995，这样当然

$$4568+7391\neq 11995.$$

但同余式 $11995\equiv 7 \pmod 9$ 还是成立．

这就是說，用定理所示的方法来檢驗加法或減法运算的正确性，有时会失效的．然而一般說来，失效的机会究竟是少的，所以定理还是有它的存在价値．

2．如果 $a\cdot b=c$，設 $a\equiv r_1 \pmod 9$，$b\equiv r_2 \pmod 9$，$c\equiv r_3 \pmod 9$，那末 $r_1\cdot r_2\equiv r_3 \pmod 9$.

証明 因为 $a\equiv r_1 \pmod 9$，$b\equiv r_2 \pmod 9$，

所以 $ab\equiv r_1 r_2 \pmod 9$.

又 $c\equiv r_3 \pmod 9$，且 $ab=c$，

因此 $r_1\cdot r_2\equiv r_3 \pmod 9$.

如果取的 r_1、r_2、r_3 是小于 9 的非負整数（即 r_1、r_2、r_3 是非負的最小剩余），那末

当 $r_1\cdot r_2<9$ 的时候，$r_1r_2=r_3$.

当 $r_1\cdot r_2\geqslant 9$ 的时候，設 r'_3 是 $r_1 r_2$ 被 9 除后的非負最小剩余，于是 $r'_3=r_3$.

例 $3748\cdot 6236=23372528$.

容易看到：$3748\equiv 4 \pmod 9$；

$6236\equiv 8 \pmod 9$；

$$23372528 \equiv 5 \pmod 9.$$

很明显，4、8、5三个数的关系是：$4\cdot 8 \equiv 5 \pmod 9$.

显然，上述定理可推广到多个数相乘的情形.

例 $64\cdot 14\cdot 25=22400$.

因为 $64 \equiv 1 \pmod 9$, $14 \equiv 5 \pmod 9$,

$25 \equiv 7 \pmod 9$, $22400 \equiv 8 \pmod 9$.

显然，1、5、7、8四个数之間的关系是：$1\cdot 5\cdot 7 \equiv 8 \pmod 9$.

我們采用上面定理的等价形式，可以檢驗乘法运算的正确与否：

設 $a \equiv r_1 \pmod 9$, $b \equiv r_2 \pmod 9$, $c \equiv r_3 \pmod 9$，如果 $r_1\cdot r_2 \not\equiv r_3 \pmod 9$，那末 $a\cdot b \neq c$.

例 檢驗 $4568\cdot 7391=30746529$ 正确与否.

因为 $4568 \equiv 5 \pmod 9$, $7391 \equiv 2 \pmod 9$，而

$$30746529 \equiv 0 \pmod 9.$$

显然，$2\cdot 5=10$，而10与0对于模数9不同余，所以上面的乘法运算不正确.

注 $r_1 r_2 \equiv r_3 \pmod 9$ 仅是 $a\cdot b=c$ 的必要条件. 也就是說，用定理所示的方法来檢驗乘法运算的正确与否，有时会失效的. 虽有这个缺陷，但因为失效的机会究竟是很少的，所以这一定理还是有它的存在价值.

关于能整除的除法运算的檢驗法，可由上面的定理导出：

設 $a \vdots b$，而 $a\div b=c$，并設 $a \equiv r_1 \pmod 9$, $b \equiv r_2 \pmod 9$, $c \equiv r_3 \pmod 9$，那末 $r_2\cdot r_3 \equiv r_1 \pmod 9$.

例 $4550\div 14=325$.

很容易看到：$4550 \equiv 5 \pmod 9$, $14 \equiv 5 \pmod 9$,

而 $325 \equiv 1 \pmod 9$，显然，$5\cdot 1 \equiv 5 \pmod 9$.

例 我們可以发現下面的除法运算是不正确的：$4567\div 23=195$.

这是因为 $4567 \equiv 4 \pmod 9$,

$23 \equiv 5 \pmod 9$,

$$195 \equiv 6 \pmod 9,$$

而 $$5 \cdot 6 \not\equiv 4 \pmod 9.$$

另外，由上面的定理也可推得对乘方运算的检驗：

如果 $a^n = b$，設 $a \equiv r_1 \pmod 9$，$b \equiv r_2 \pmod 9$，那末 $r_1^n \equiv r_2 \pmod 9$.

例 $13^4 = 28561$ 正确与否？

我們說上面的运算是正确的①．这是因为 $28561 \equiv 4 \pmod 9$. 而 $13 \equiv 4 \pmod 9$，所以 $13^4 \equiv 4^4 \equiv 4 \pmod 9$. 因此 $13^4 = 28561$.

例 $7^5 = 98117$ 正确与否？

因为 $7^2 \equiv 4 \pmod 9$，于是 $7^4 \equiv 4^2 \equiv 7 \pmod 9$，所以

$$7^5 \equiv 49 \equiv 4 \pmod 9.$$

另一方面，$98117 \equiv 8 \pmod 9$.

因此可以說，$7^5 \neq 98117$.

可以看出，如果 $a = 9k$（k是整数），检驗起来最为方便．

3．如果 $$A = BQ + R \quad (0 < R < B),$$

又設

$$A \equiv r_1 \pmod 9, \tag{1}$$

$$B \equiv r_2 \pmod 9, \tag{2}$$

$$Q \equiv r_3 \pmod 9, \tag{3}$$

$$R \equiv r_4 \pmod 9, \tag{4}$$

那末 $$r_2 r_3 + r_4 \equiv r_1 \pmod 9.$$

証明 由(2)、(3)知：$BQ \equiv r_2 r_3 \pmod 9$. 而$R \equiv r_4 \pmod 9$，所以

$$BQ + R \equiv r_2 r_3 + r_4 \pmod 9.$$

而 $A \equiv r_1 \pmod 9$，因此得：

$$r_2 r_3 + r_4 \equiv r_1 \pmod 9.$$

例 計算 339 除以 13，得 $339 = 13 \cdot 26 + 1$.

因为 $339 \equiv 6 \pmod 9$，$13 \equiv 4 \pmod 9$，

---

① 显然，这样断定，也是欠严格的．因为 $r_1^n \equiv r_2 \pmod 9$ 也仅是 $a^n = b$ 的必要条件．

$$26 \equiv 8 \pmod 9, \quad 1 \equiv 1 \pmod 9,$$

显然，
$$4 \cdot 8 + 1 \equiv 6 \pmod 9.$$

例 檢驗 $45698 = 234 \cdot 298 + 46$ 正确与否.

因为
$$45698 \equiv 5 \pmod 9,$$
$$234 \equiv 0 \pmod 9,$$
$$298 \equiv 1 \pmod 9,$$
$$46 \equiv 1 \pmod 9,$$

而
$$0 \cdot 1 + 1 \not\equiv 5 \pmod 9,$$

所以
$$45698 \neq 234 \cdot 298 + 46.$$

注 这里 $r_2 r_3 + r_4 \equiv r_1 \pmod 9$ 也仅是 $A = BQ + R$ 的必要条件.

这一节中，各条定理都是以 9 为模数的.我們不难发现在証明过程中根本沒有用到"9"的特殊性质，这就表示这些定理是可以用任意正整数为模数的.至于所以要用 9 作为模数，一方面因为計算某数被 9 除后所得的余数比較方便；另一方面，对保証檢驗的可靠性上起了一些作用.这是因为計算某数被 9 除后的余数要牵涉到这个数的每一位数字.（例如采用 2、10 作为模数，求余数时就只与某数的末一位数碼有关.也就是說，只要末位数字相同的数，它們被 2 或 10 除后余数总是相等的.）

如果用 11 作为模数也符合上述的条件，当然我們也可以把上面那些定理中的模数换成 11（况且有时的确会覺得方便）.

例 檢驗 $4568 \cdot 7391 = 30746529$ 正确与否.

因为
$$4568 \equiv 8 - 6 + 5 - 4 = 3 \pmod{11},$$
$$7391 \equiv 1 - 9 + 3 - 7 \equiv 10 \pmod{11},$$
$$30746529 \equiv 9 - 2 + 5 - 6 + 4 - 7 + 0 - 3 = 0 \pmod{11},$$

事实上，$3 \cdot 10 \not\equiv 0 \pmod{11}$，所以这个乘法运算不正确.

§5 剩余类 · 完全剩余組

定义 对于模数 m 同余的一切数的集合，就叫做以 m 为模数的剩余类.

例 如下的数的集合，就是一个以 7 为模数的剩余类：

……，$7(-3)+3$，$7(-2)+3$，$7(-1)+3$，$7\cdot0+3$，$7\cdot1+3$，$7\cdot2+3$，$7\cdot3+3$，…….

也就是 ……，-18，-11，-4，3，10，17，24，…….

定理 对于模数 m，存在而且只存在 m 个相异的剩余类.

証明 因为一切整数被 m 除后的非負最小剩余不外是：0、1、2、3、……、$m-1$ 这 m 个数，所以存在 m 个相异的剩余类，每一个剩余类中一切数的一般形式可表示如下：

$$mt+0;$$
$$mt+1;$$
$$\cdots\cdots;$$
$$mt+(m-1).$$
$$(t=0、\pm1、\pm2、\cdots\cdots)$$

如果还存在一剩余类，設其中一切数的一般形式是 $mt+k$. 我們有理由設 $k=mq+r$ $(0\leqslant r<m)$，于是 $mt+k=m(t+q)+r$.

因为 $0\leqslant r<m$，而 $t+q$ 仍然是整数，所以該剩余类无非是指出的 m 个中的一个.

定理 一个模数 m 的剩余类里的一切数，它們与 m 的最大公約数都相等.

証明 設 a、b 是以 m 为模的剩余类里的任意两数，就是說 $a\equiv b \pmod m$. 我們要証明：

$$(|a|,\ m)=(|b|,\ m).$$

設 $a=mq_1+r_1$ $(0\leqslant r_1<m)$，$b=mq_2+r_2$ $(0\leqslant r_2<m)$，于是：

$$(|a|,\ m)=(m,\ r_1),\quad (|b|,\ m)=(m,\ r_2).$$

由所設知 $r_1=r_2$，因此得 $(|a|,\ m)=(|b|,\ m)$.

下面討論完全剩余組問題.

定义 在 m 个以 m 为模的相异的剩余类中，各取一个数，这样得到的 m 个数，叫做以 m 为模数的一个完全剩余組. 例如，0、1、2、……、

$m-1$ 这 m 个数，就是模 m 的完全剩余組．通常把上面的这个数組，叫做模 m 的非負最小剩余組．又如，0、-1、-2、……、$-(m-1)$这个数組，也是模 m 的完全剩余組．通常把上面的数組叫做模 m 的最小負剩余組（就是說，絕对值是非負最小的剩余組）．

例 当 m 是奇数的时候，下面的 m 个数构成了模 m 的完全剩余組：

$$0、\pm 1、\pm 2、\cdots\cdots、\pm\frac{m-1}{2}.$$

当 m 是偶数的时候，下面的 m 个数构成了模 m 的完全剩余組：

$$-\frac{m}{2}+1、-\frac{m}{2}、\cdots\cdots、-1、0、1、\cdots\cdots、\frac{m}{2};$$

或 $$-\frac{m}{2}、\cdots\cdots、-1、0、1、\cdots\cdots、\frac{m}{2}、\frac{m}{2}+1.$$

以上所得到的模 m 的完全剩余組，也叫做絕对最小剩余組（也就是說，絕对值最小的剩余組）．

根据定义直接可以推知：有 m 个数，如果其中任意两个对于模 m 都不同余，那末这 m 个数构成模 m 的完全剩余組．

事实上，这 m 个数恰好是分別属于以 m 为模数的 m 个相异的剩余类内．

定理 設 a 是非零整数，b 是任意整数，且$(|a|, m)=1$，如果 t 通过模 m 的完全剩余組內的一切数，那末形如 $at+b$ 的数必构成一个以 m 为模数的完全剩余組．

証明 設 t_1、t_2 为模 m 的完全剩余組內的任意两数（当然它們对于模 m 是不同余的）．

現在要証明 at_1+b 与 at_2+b 对于模 m 不同余（如果証明了这点，也就是說：形如 $at+b$ 的 m 个数对于模 m，沒有两个是同余的．这就証实了定理是成立的）．

假定 $at_1+b\equiv at_2+b \pmod{m}$，根据 §2.1 的推論可得：

$$at_1\equiv at_2 \pmod{m}.$$

因为($|a|$, m)，所以根据 §2 4 可得：

$$t_1 \equiv t_2 \pmod{m}.$$

显然，这与所設 t_1、t_2 对模 m 是不同余的这一点相違背．既然这样，也就証明了定理成立．

特别的，当 $b=0$ 的时候，定理变成如下的形式：如果$(|a|, m)=1$，且 t 通过模 m 的完全剩余組内的一切数，形如 at 的 m 个数构成一个模 m 的完全剩余組．

例 1 如果 k 是一个整数，那末 k、$k+1$、$k+2$、……、$k+m-1$ 等数构成了模 m 的完全剩余組．

上面的断言，虽可直接根据定义来証明，事实上，它可由上面的定理直接推得：

只要取 $a=1$，$b=k$，而 t 通过 0、1、2、……、$m-1$．

于是說：連續的 m 个整数，必构成模 m 的完全剩余組．

例 2 如果 $(|a|, m)=1$，那末 0、a、$2a$、……、$(m-1)a$ 构成模 m 的完全剩余組．

上面的断言，可由定理直接推得：

只要取 $b=0$，而 t 通过 0、1、2、……、$m-1$．

例 3 設$(|a|, m)=1$，b 是任一整数，又設 $ax+b\equiv r_x \pmod{m}$ $(0\leqslant r_x<m)$，那末，当 x 通过模 m 的完全剩余組内的一切数的时候，

$$\sum_x \frac{r_x}{m}=\frac{1}{2}(m-1).$$

証明 因为 r_x 是 $ax+b$ 对于模 m 的非負最小剩余，而当 x 通过模 m 的完全剩余組内的一切数的时候，$ax+b$ 也通过了模 m 的完全剩余組内的一切数．所以当 x 通过模 m 的完全剩余組内的一切数的时候，r_x 通过了 0、1、2、……、$m-1$．

于是

$$\sum_x \frac{r_x}{m}=\frac{0}{m}+\frac{1}{m}+\cdots\cdots+\frac{m-1}{m}$$

$$=\frac{1}{m}[1+2+\cdots\cdots+(m-1)]$$

$$=\frac{1}{2}(m-1).$$

例4 設 m_1、m_2、……、m_k 是正整数，x_1、x_2、……、x_k 分别独立地通过模 m_1、m_2、……、m_k 的完全剩余組内的一切数，那末

$$x_1+m_1x_2+m_1m_2x_3+\cdots\cdots+m_1m_2\cdots\cdots m_{k-1}x_k \tag{1}$$

构成了模 $m_1m_2\cdots\cdots m_k$ 的完全剩余組.

証明 我們应該証明以下两点.

1. (1)表示 $m_1m_2\cdots\cdots m_k$ 个数；

2. 形如(1)的任意两个数，对于模 $m_1m_2\cdots\cdots m_k$ 都不同余.

关于1的成立很明显：

因为在(1)中 x_1 代表着 m_1 个不同的数；

x_2 代表着 m_2 个不同的数；

……………………………；

x_k 代表着 m_k 个不同的数.

要証明2，也只需証明：

当 $x_1=p_1$，$x_2=p_2$，……，$x_k=p_k$ 的时候，(1)的值与当 $x_1=q_1$，$x_2=q_2$，……，$x_k=q_k$ 的时候，(1)的值对于模 $m_1m_2\cdots\cdots m_k$ 不同余.

(这里 $0\leqslant p_i<m_i$，$0\leqslant q_i<m_i$，且在 p_1、q_1；p_2，q_2；……；p_k、q_k 中至少有一对不相等.)

假定 $p_1+m_1p_2+m_1m_2p_2+\cdots\cdots+m_1m_2\cdots\cdots m_{k-1}p_k$

$\equiv q_1+m_1q_2+m_1m_2q_3+\cdots\cdots+m_1m_2\cdots\cdots m_{k-1}q_k \pmod{m_1m_2\cdots\cdots m_k}$.

那末 $p_1-q_1\equiv m_1Q_1 \pmod{m_1m_2\cdots\cdots m_k}$.(这里 Q_1 是整数)

因为同余式的右边与模都能被 m_1 整除，所以 $p_1-q_1 \vdots m_1$.

又 $0\leqslant p_1<m_1$，$0\leqslant q_1<m_1$，所以 $p_1=q_1$.

这样就有同余式：

$$m_1p_2+m_1m_2p_3+\cdots\cdots+m_1m_2\cdots\cdots m_{k-1}p_k$$
$$\equiv m_1q_2+m_1m_2q_3+\cdots\cdots+m_1m_2\cdots\cdots m_{k-1}q_k \pmod{m_1m_2\cdots\cdots m_k}.$$

于是得 $m_1(p_2-q_2)\equiv m_1m_2Q_2 \pmod{m_1m_2\cdots\cdots m_k}$.(这里 Q_2 是整数)

也就是 $$p_2-q_2\equiv m_2Q_2 \pmod{m_2m_3\cdots\cdots m_k}.$$

因为同余式的右边及模都能被 m_2 整除,所以 $p_2-q_2 \vdots m_2$.

又 $0\leqslant p_2<m_2$, $0\leqslant q_2<m_2$, 所以 $p_2=q_2$.

依次类推,最后得

$$m_1m_2\cdots\cdots m_{k-1}p_k\equiv m_1m_2\cdots\cdots m_{k-1}q_k \pmod{m_1m_2\cdots\cdots m_k}.$$

因而 $$p_k\equiv q_k \pmod{m_k}.$$

因为 $0\leqslant p_k<m_k$, $0\leqslant q_k<m_k$, 所以 $p_k=q_k$.

上面的結果,就与"p_1、q_1; p_2、q_2; ……; p_k、q_k; 至少有一对不相等"这一前提矛盾.

于是;就証明了形如(1)的 $m_1m_2\cdots\cdots m_k$ 个数,确是构成了模 $m_1m_2\cdots\cdots m_k$ 的完全剩余組.

特别的,当 $m_1=m_2=\cdots\cdots=m_k$ 的时候,定理变成如下的形式:

如果 x_1、x_2、……、x_k 独立地通过模 m 的完全剩余組,那末形如 $x_1+mx_2+\cdots\cdots+m^{k-1}x_k$ 的数,构成了模 m^k 的完全剩余組.

下面我們考察一个具体例子:如果 x_1、x_2 独立地通过模 4 的完全剩余組,那末根据上述的結果可知,形如

$$x_1+4x_2 \tag{1}$$

的数构成模 4^2 的完全剩余組.

取模 4 的完全剩余組是:0、1、2、3.

当 $x_1=0$, x_2 通过 0、1、2、3 的时候,(1)呈现出:

0、 4、 8、 12;

当 $x_1=1$, x_2 通过 0、1、2、3 的时候,(1)呈现出:

1、 5、 9、 13;

当 $x_1=2$, x_2 通过 0、1、2、3 的时候,(1)呈现出:

$$2、\ 6、\ 10、\ 14;$$

当 $x_1=3$, x_2 通过 0、1、2、3 的时候,(1)呈现出:

$$3、\ 7、\ 11、\ 15.$$

我們观察所得的16个数,发现它們正好构成了模16的完全剩余組.

例5 設 m_1、m_2、……、m_k 是两两互質的数,又設 $m_1m_2\cdots\cdots m_k=m_1\cdot M_1=m_2\cdot M_2=\cdots\cdots=m_k\cdot M_k$. 如果 x_1、x_2、……、x_k 分别独立地通过模 m_1、m_2、……、m_k 的完全剩余組,那末形如

$$M_1x_1+M_2x_2+\cdots\cdots+M_kx_k \tag{1}$$

的数,构成模 $m_1m_2\cdots\cdots m_k$ 的完全剩余組.

証明 形如(1)的数共有 $m_1m_2\cdots\cdots m_k$ 个是不需要再証明的. 我們只要証明:任意两个形如(1)的数,对于模 $m_1m_2\cdots\cdots m_k$ 都不同余.

假定 $M_1p_1+M_2p_2+\cdots\cdots+M_kp_k$

$$\equiv M_1q_1+M_2q_2+\cdots\cdots+M_kq_k \pmod{m_1m_2\cdots\cdots m_k}. \tag{2}$$

(这里 $0\leqslant p_i<m_i$, $0\leqslant q_i<m_i$, 且 p_1, q_1; p_2, q_2; ……; p_n, q_n 中至少有一对不相等.)

于是得

$$M_1(p_1-q_1)\equiv M_2(q_2-p_2)+\cdots\cdots+M_k(q_k-p_k) \pmod{m_1m_2\cdots m_k}.$$

注意一下 M_1、M_2、……、M_k 等数的意义,就可知道:除 M_1 外,M_2、M_3、……、M_k 各数都能被 m_1 整除.

这就說明了这个同余式的右边及模都能被 m_1 整除,所以

$$M_1(p_1-q_1)\,\vdots\, m_1.$$

因为 $M_1=m_2m_3\cdots\cdots m_k$, 当然 $(M_1,\ m_1)=1$, 所以 $p_1-q_1\,\vdots\, m_1$. 又 $0\leqslant p_1<m_1$, $0\leqslant q_1<m_1$, 因此 $p_1=q_1$.

这样,(2)就变成:

$$M_2p_2+\cdots\cdots+M_kp_k\equiv M_2q_2+\cdots\cdots+M_kq_k \pmod{m_1m_2\cdots\cdots m_k}.$$

同理可証, $p_2=q_2$.

依次类推,可得 $p_3=q_3$; ……; $p_k=q_k$.

这就与“在 p_1, q_1; p_2, q_2; ……; p_n, q_n 中至少有一对不相等”的假設矛盾了.

于是就証实了,形如(1)的 $m_1m_2\cdots\cdots m_k$ 个数确組成了模 $m_1m_2\cdots\cdots m_k$ 的完全剩余組.

讀者可驗証:設 $m_1=4$、$m_2=5$, 当 x_1、x_2 分别独立地通过模 4、5 的完全剩余組时,形如 $5x_1+4x_2$ 的数,构成模 $4\cdot5$ 的完全剩余組.

§6 欧拉函数

定义 符号 $\phi(N)$,表示不大于正整数 N,而与 N 互質的数的个数. $\phi(N)$ 叫做欧拉函数.

例如,在不大于 12 的数中,与 12 互質的数有 1、5、7、11 四个,因此 $\phi(12)=4$.

又如,在不大于 11 的数中,与 11 互質的数有 1、2、……、10 十个,因此 $\phi(11)=10$.

很明显,如果 N 是質数, $\phi(N)=N-1$.

如果 N 是合数,要求 $\phi(N)$, 应先解决下面几条定理.

定理 1 如果 $(a, b)=1$, 那末 $\phi(ab)=\phi(a)\cdot\phi(b)$.

証明 $\phi(ab)$ 就是表示不大于 ab, 而与 ab 互質的数的个数. 但是与 ab 互質的数, 一定既与 a 互質, 又与 b 互質. 反过来, 也成立(参閱第一章 §2 性質 11 的推論 2). 于是, $\phi(ab)$ 是在不大于 ab 的一切数中,既与 a 互質,又与 b 互質的数的个数.

我們把 1 到 ab 之間的数,按照 a 列 b 行排列:

$$\begin{array}{ccccc}
1 & 2 & 3 & \cdots\cdots & a \\
a+1 & a+2 & a+3 & \cdots\cdots & a+a \\
2a+1 & 2a+2 & 2a+3 & \cdots\cdots & 2a+a \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
(b-2)a+1 & (b-2)a+2 & (b-2)a+3 & \cdots\cdots & (b-2)a+a \\
(b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \cdots\cdots & (b-1)a+a
\end{array}$$

我們考察其中任意一列：

$$k,\ a+k,\ 2a+k,\ \cdots\cdots,\ (b-2)a+k,\ (b-1)a+k.\ (1\leqslant k\leqslant a)$$

在这列数中，每一个数都与 a 互质或不互质是决定于 k 这个数与 a 互质还是不互质[如果 $(k,\ a)=d$，那末

$$(a+k,\ a)=(k,\ a)=d;$$

$$(2a+k,\ a)=(k,\ a)=d;$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots;$$

$$(b-1)a+k,\ a)=(k,\ a)=d].$$

然而已經知道，1、2、……、a 这些数中与 a 互质的有且仅有 $\phi(a)$ 个. 所以如上安排的 a 列数中，有且仅有 $\phi(a)$ 列数与 a 互质.

再来研究这 $\phi(a)$ 列与 a 互质的数中，与 b 互质的数的个数. 我們用

$$t,\ a+t,\ 2a+t,\ \cdots\cdots,\ (b-2)a+t,\ (b-1)a+t \qquad (1)$$

代替 $\phi(a)$ 列与 a 互质中的任意一列。

已知这些数中 $(a,\ b)=1$，根据 §5 的定理可知这 b 个数就是模 b 的完全剩余組。

我們用 b 去除(1)中的数，把得到的余数整理一下，就成为下面的一組数：

$$0、1、2、\cdots\cdots、b-1. \qquad (2)$$

因此要計算(1)中有几个数与 b 互质，就只要去計算(2)中有几个数与 b 互质[对于正整数 A、B，如果 $A=BQ+R\ (0<R<B)$，那末要观察 B 与 A 是否互质，只需观察 B 与 R 是否互质. 这是因为 $(A,\ B)=(B,\ R)$].

于是(1)中与 b 互质的数有且仅有 $\phi(b)$ 个.

既然在 $\phi(a)$ 列数中，每一列与 b 互质的数有且仅有 $\phi(b)$ 个，因此 $\phi(a)$ 列中与 b 互质的数有且仅有 $\phi(a)\cdot\phi(b)$ 个. 当然这 $\phi(a)\cdot\phi(b)$ 个数也就是不大于 ab，且与 a 互质又与 b 互质的数了.

所以 $$\phi(ab)=\phi(a)\cdot\phi(b).$$

上面的定理容易推广如下：

如果 $a_1, a_2, \cdots\cdots, a_n$ 各数中两两互质，那末

$$\phi(a_1a_2\cdots\cdots a_n)=\phi(a_1)\cdot\phi(a_2)\cdot\cdots\cdots\cdot\phi(a_n).$$

定理 2 設 $N=a^p$，这里 a 是質数，那末

$$\phi(N)=a^p\left(1-\frac{1}{a}\right).$$

証明 首先研究，在

$$1, 2, 3, \cdots\cdots, a^p-1, a^p \tag{1}$$

这 a^p 个数中，有几个数与 a^p 不互質.

显然，与 a 不互質的数一定与 a^p 也不互質；反过来，与 a^p 不互質的也一定与 a 不互質[如果与 a^p 不互質的数 k 与 a 互質，就是 $(k, a)=1$，那末由互質数的性質知 $(k, a^p)=1$，这就有了矛盾]。

于是，要計算(1)中有几个数与 a^p 不互質，就只需計算这些数中有几个数与 a 不互質.

很清楚的可以看到，在(1)中有且仅有下列一些数与 a 不互質(注意 a 是質数)：

$$a, 2a, 3a, \cdots\cdots, (a^{p-1}-1)a, (a^{p-1})a.$$

就是說，在(1)中有且仅有 a^{p-1} 个数与 a 不互質，也就是有且仅有 a^{p-1} 个数与 a^p 不互質。

不大于 a^p 的数共有 a^p 个，其中有 a^{p-1} 个与它不互質，当然剩下的 a^p-a^{p-1} 个就与它互質了.

因此
$$\phi(a^p)=a^p-a^{p-1}=a^p\left(1-\frac{1}{a}\right).$$

例 $\phi(5^5)=5^5-5^4=5^4\cdot 4=2500$。

定理 3 如果 $N=a_1^{\alpha_1}a_2^{\alpha_2}\cdots\cdots a_n^{\alpha_n}$，(这里 $a_1, a_2, \cdots\cdots, a_n$ 是相异質数)那末

$$\phi(N)=N\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\cdots\cdots\left(1-\frac{1}{a_n}\right).$$

証明 根据互质数的性质，可推知：$a_1^{\alpha_1}, a_2^{\alpha_2}, \cdots\cdots, a_n^{\alpha_n}$ 是两两互质的（因为 a_1、a_2、……、a_n 显然是两两互质的）．于是由定理1、2，得

$$\begin{aligned}\phi(N)&=\phi(a_1^{\alpha_1}a_2^{\alpha_2}\cdots\cdots a_n^{\alpha_n})\\&=\phi(a_1^{\alpha_1})\cdot\phi(a_2^{\alpha_2})\cdots\cdots\cdot\phi(a_n^{\alpha_n})\\&=a_1^{\alpha_1}\left(1-\frac{1}{a_1}\right)\cdot a_2^{\alpha_2}\left(1-\frac{1}{a_2}\right)\cdots\cdots a_n^{\alpha_n}\left(1-\frac{1}{a_n}\right)\\&=(a_1^{\alpha_1}a_2^{\alpha_2}\cdots\cdots a_n^{\alpha_n})\cdot\left(1-\frac{1}{a_1}\right)\cdot\left(1-\frac{1}{a_2}\right)\cdots\cdots\cdot\left(1-\frac{1}{a_n}\right)\\&=N\left(1-\frac{1}{a_1}\right)\cdot\left(1-\frac{1}{a_2}\right)\cdots\cdots\cdot\left(1-\frac{1}{a_n}\right).\end{aligned}$$

这个求得的公式叫做高斯公式．

例1 如果 $N=600$，求 $\phi(N)$．

因为 $600=2^3\cdot3\cdot5^2$，所以

$$\begin{aligned}\phi(N)&=600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\&=\frac{600\cdot1\cdot2\cdot4}{2\cdot3\cdot5}\\&=160.\end{aligned}$$

例2 如果 $N=66150$，求 $\phi(N)$．

因为 $66150=2\cdot3^3\cdot5^2\cdot7^2$，

所以 $\phi(N)=2\cdot3^3\cdot5^2\cdot7^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$

$$\begin{aligned}&=\frac{2\cdot3^3\cdot5^2\cdot7^2\cdot2\cdot4\cdot6}{2\cdot3\cdot5\cdot7}\\&=15120.\end{aligned}$$

現在，求 $\phi(N)$ 的問題解决了．下面几个定理指出了欧拉函数的一些性质．

定理1 如果 $N>2$，那末 $\phi(N)$ 一定是偶数．

証明 如果 N 是质数，那末 $\phi(N)=N-1$. 而所有大于 2 的质数一定是奇数，所以 $N-1$ 是偶数. 也就是說，当 N 取质数时，論断成立.

如果 N 是合数，我們設

$$N=a_1^{\alpha_1}a_2^{\alpha_2}\cdots\cdots a_n^{\alpha_n}\ (a_1,\ a_2,\ \cdots\cdots,\ a_n\ 是相异的质数),$$

那末 $\qquad \phi(N)=\phi(a_1^{\alpha_1})\cdot\phi(a_2^{\alpha_2})\cdots\cdots\cdot\phi(a_n^{\alpha_n}).$

观察 $\qquad \phi(a_k^{\alpha_k}),\ (k=1,\ 2,\ \cdots\cdots,\ n)$

因为 $\phi(a_k^{\alpha_k})=a_k^{\alpha_k}-a_k^{\alpha_k-1}=a_k^{\alpha_k-1}(a_k-1)$, 已知 a_k 是质数，如果 $a_k=2$. $\phi(a_k^{\alpha_k})$就显然是偶数.

如果 $a_k>2$, 当然 a_k 一定是奇数，所以 a_k-1 是偶数. 也就是說，$\phi(a_k^{\alpha_k})$是偶数.

这就証明了 $\phi(N)$ 实在是 n 个偶数的乘积，因此 $\phi(N)$ 一定是偶数.

定理 2 不大于N，且与N互质的一切数，它們的和是$\frac{1}{2}N\cdot\phi(N)$.

証明 如果 $N=2$, $\phi(N)=\phi(2)=1$, 那末$\frac{1}{2}N\cdot\phi(N)=\frac{1}{2}\cdot2\cdot1=1$. 另一方面不大于 2 且与 2 互质的数它們的和也确是 1. 因此当 $N=2$ 的时候，定理成立.

下面对于 $N>2$ 的一般情形加以証明.

先注意这样的情形：

如果数 $x<N$, 且 $(N,\ x)=1$, 当然可以得到 $(N-x,\ N)=1$ (显然，$N-x<N$).

将不大于 N，且与 N 互质的 $\phi(N)$个数，按由小到大的順序排列. 如果前$\frac{1}{2}\phi(N)$① 个数，我們用

$$1,\ \mu_2,\ \mu_3,\ \cdots\cdots,\ \mu_{k-1},\ \mu_k\ \left[这里,\ k=\frac{1}{2}\phi(N)\right]$$

表示. 那末后$\frac{1}{2}\phi(N)$个数，一定順次是：

---

① $\because$ $N>2$ 时，$\phi(N)$必是偶数，故$\frac{1}{2}\phi(N)$为整数.

$$N-\mu_k,\ N-\mu_{k-1},\ \cdots\cdots,\ N-\mu_3,\ N-\mu_2,\ N-1.$$

設不大于 N，且与 N 互質的一切数的总和是 S，那末

$$S=1+\mu_2+\mu_3+\cdots\cdots+\mu_k$$
$$+(N-\mu_k)+\cdots\cdots+(N-\mu_2)+(N-1).$$

在这 $\phi(N)$ 个数的和中，与首尾等距的两个数的和都是 N，于是得到：

$$S=N+N+\cdots\cdots+N\quad \left[\text{項数是}\frac{1}{2}\phi(N)\right]$$

$$=N\cdot\frac{1}{2}\phi(N)=\frac{1}{2}N\cdot\phi(N).$$

例1 求不大于 600，且与 600 互質的一切数的和.

$$S=\frac{1}{2}\cdot 600\cdot\phi(600)。\text{而 } \phi(600)=160,$$

所以 $$S=300\cdot 160=48000.$$

例2 求不大于 A^n（A 是質数），且与 A^n 互質的一切数的和.

$$S=\frac{1}{2}A^n\cdot\phi(A^n)=\frac{1}{2}A^n(A^n-A^{n-1})=\frac{1}{2}(A^{2n}-A^{2n-1}).$$

对于欧拉函数，最后給出如下的定理.

首先規定下面記号的意义：

記号 $\sum\limits_{d\setminus N}$，表示对 N 的約数 d 展开的和式.

譬如，$N=8$，那末

$$\sum_{d\setminus N}f(d)=f(1)+f(2)+f(4)+f(8).$$

定理 如果 $N=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\cdots\cdots\cdot p_n^{\alpha_n}$，（$p_1$、$p_2$、……、$p_n$ 是相异的質数）那末

$$\sum_{d\setminus N}\phi(d)=N.$$

証明 先看一个特殊情形：

如果 $N=p_1^{\alpha_1}$，求証：$\sum\limits_{d\setminus N}\phi(d)=p_1^{\alpha_1}$.

因为 d 具有形式 $p_1^{\beta_1}$ $(0\leqslant\beta_1\leqslant\alpha_1)$，所以

$$\sum_{d\setminus N}\phi(d)=\sum_{0\leq\beta_1\leq\alpha_1}\phi(p_1^{\beta_1})$$

$$=\phi(p_1^0)+\phi(p_1^1)+\cdots\cdots+\phi(p_1^{\alpha_1})$$

$$=1+(p_1-1)+(p_1^2-p_1)+\cdots\cdots+(p_1^{\alpha_1}-p_1^{\alpha_1-1})$$

$$=p_1^{\alpha_1}.$$

下面再証明一般情形:

因为 d 具有形式 $p_1^{\beta_1}p_2^{\beta_2}\cdot\cdots\cdots\cdot p_n^{\beta_n}$ $(0\leqslant\beta_i\leqslant\alpha_i,\ i=1、2、\cdots\cdots、n)$, 所以

$$\sum_{d\setminus N}\phi(d)=\sum_{0\leq\beta_1\leq\alpha_1,\ \cdots\cdots,\ 0\leq\beta_n\leq\alpha_n}\phi(p_1^{\beta_1}p_2^{\beta_2}\cdot\cdots\cdots p_n^{\beta_n}).$$

已知 $\phi(p_1^{\beta_1}p_2^{\beta_2}\cdot\cdots\cdots\cdot p_n^{\beta_n})=\phi(p_1^{\beta_1})\cdot\phi(p_2^{\beta_2})\cdot\cdots\cdots\cdot\phi(p_n^{\beta_n})$, 所以

$$\sum_{d\setminus N}\phi(d)=\sum_{0\leq\beta_2\leq\alpha_1}\phi(p_2^{\beta_1})\cdot\sum_{0\leq\beta_2\leq\alpha_2}\phi(p_1^{\beta_2})\cdot\cdots\cdots\cdot\sum_{0\leq\beta_n\leq\alpha_n}\phi(p_n^{\beta_n}).①$$

因为

$$\sum_{0\leq\beta_1\leq\alpha_1}\phi(p_1^{\beta_1})=p_1^{\alpha_1},$$

$$\sum_{0\leq\beta_2\leq\alpha_2}\phi(p_2^{\beta_2})=p_2^{\alpha_2},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\sum_{0\leq\beta_n\leq\alpha_n}\phi(p_n^{\beta_n})=p_n^{\alpha_n},$$

所以 $$\sum_{d\setminus N}\phi(d)=p_1^{\alpha_1}p_2^{\alpha_2}\cdot\cdots\cdots\cdot p_n^{\alpha_n}=N.$$

例　如果 $N=12$, 我們求得:

---

① 如 $\sum_{1\leq i\leq m,\ 1\leq j\leq n}(a_ib_j)=\sum_{1\leq i\leq m}a_i\cdot\sum_{1\leq j\leq n}b_j.$

因为　右边$=(a_1+a_2+\cdots\cdots+a_m)(b_1+b_2+\cdots\cdots+b_n)$, 展开后的和式中, 每一項都有形式 a_ib_j, 这里 i、j 分别独立地通过 1、2、……、m 及 1、2、……、n.

$$\sum_{d\backslash N}\phi(d)=\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12)$$

$$=1+1+2+2+2+4=12.$$

§7 与模互質的剩余組

我們已經知道对于模 m 有 m 个相异的剩余类存在.

定义 在这 m 个相异的剩余类中，一定能找出一組剩余类，这組剩余类中的任一个，它里面的所有数，按絕对值説都与 m 互質（由 §5 的定理可知：在一个剩余类内所有的数中，只要发現有一个数与 m 互質，就表示这剩余类里的一切数都与 m 互質），而除了这組以外的其它任意一个剩余类，它里面的所有数，按絕对值説都与 m 不互質．从这样的一組剩余类里，各取出一个数来，所构成的一組数叫做与模 m 互質的剩余組.

由定义可知，与模 m 互質的剩余組，就是由模 m 的完全剩余組里，与模 m 互質的数所构成的.

例如，0、1、2、……、12、13 这些数是模 14 的完全剩余組；而 1、3、5、9、11、13 这些数就是与模 14 互質的剩余組.

容易証明：与模 m 互質的剩余組含有且仅含有 $\phi(m)$ 个数.

証明留給讀者.

例 $\because\ \phi(200)=\phi(2^3)\cdot\phi(5^2)$

$$=200\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=80,$$

所以可以断言：与模 200 互質的剩余組所含的数有且仅有 80 个.

对于与模 m 互質的剩余組，也具有与模 m 的完全剩余組相类似的性質.

定理 1 如果有 $\phi(m)$ 个整数，其中任意两个，对于模 m 都不同余，且每个数都与 m 互質；那末这 $\phi(m)$ 个数构成一个与模 m 互質的剩余組.

証明 我們知道,在模 m 的 m 个相异的剩余类中,有且仅有 $\phi(m)$ 个剩余类,其中每一个里面的一切数都与 m 互质. 由已知的条件看来,这 $\phi(m)$ 个整数恰好就是从 $\phi(m)$ 个剩余类中各取一数所成的集合.于是由定义可知:这 $\phi(m)$ 个数构成了一个与模 m 互质的剩余組.

定理 2 設 $(|a|, m)=1$, 当 t 通过与模 m 互质的剩余組里的一切数的时候,形如 at 的数,一定构成一个与模 m 互质的剩余組.

証明 設 t 通过与模 m 互质的剩余組里的 $\phi(m)$ 个数,就是对应着 $\phi(m)$ 个 at 的值.現在我們只需証明:所得到的 $\phi(m)$ 个 at 的値,按絕对値說都与 m 互质,且对于 m 都是不同余的.

設 t_1、t_2 为与模 m 互质的剩余組里的任意两数[当然 $(|t_1|, m)=1$, $(|t_2|, m)=1$, 且 t_1、t_2 对于 m 不同余].

于是我們說,$|at_1|$、$|at_2|$ 也一定与 m 互质,且对于 m 也不同余.

如果 $(|at_1|, m)=d>1$, 由 $(|a|, m)=1$ 得: $(|t_1|, m)=d$. 这就与 $(|t_1|, m)=1$ 矛盾. 所以 $(|at_1|, m)=1$.

同理可証 $(|at_2|, m)=1$.

同时,如果 $at_1\equiv at_2 \pmod m$, $\because$ $(|a|, m)=1$, 根据 §2 4 得: $t_1\equiv t_2 \pmod m$. 这又与"t_1、t_2 对于 m 不同余"的假設矛盾了,所以 at_1、at_2 对于 m 不同余.

綜合上述,即証明了:当 t 通过了与模 m 互质的剩余組时,形如 at $[(|a|, m)=1]$ 的数构成一个与模 m 互质的剩余組.

例 1 設 $(|a|, m)=1$, 又設 $ax\equiv r_x \pmod m$, $(0\leqslant r_x<m)$那末当 x 通过与模 m 互质的剩余組时,

$$\sum_x \frac{r_x}{m}=\frac{1}{2}\phi(m).$$

証明 因为 x 通过与模 m 互质的剩余組,也就是說,形如 ax 的数构成了与模 m 互质的剩余組.

因为 r_x 是 ax 对于模 m 的非負最小剩余,所以当 x 通过了与模 m 互质的剩余組时,r_x 通过了 1、2、3、……、m 中一切与 m 互质的数

[共 $\phi(m)$ 个].

这样, $\sum_x r_x$ 就表示一切与 m 互质的数的和.

由上节定理知:

$$\sum_x r_x=\frac{1}{2}m\,\phi(m).$$

因此, $$\sum_x \frac{r_x}{m}=\frac{1}{m}\sum_x r_x=\frac{1}{2}\phi(m).$$

例 2 設 m_1、m_2、……、m_k 是两两互質的数, 又設 $m_1m_2\cdots\cdots m_k=m_1M_1=m_2M_2=\cdots\cdots=m_kM_k$, 如果 x_1、x_2、……、x_k 分别独立地通过与模 m_1、m_2、……、m_k 互質的剩余組, 那末形如

$$M_1x_1+M_2x_2+\cdots\cdots+M_kx_k \tag{1}$$

的数构成了与模 $m_1m_2\cdots\cdots m_k$ 互質的剩余組.

証明 我們只需証明如下的几点:

1. 形如(1)的数,有 $\phi(m_1m_2\cdots\cdots m_k)$ 个;

2. 一切形如(1)的数,对模 $m_1m_2\cdots\cdots m_k$ 都不同余;

3. 一切形如(1)的数,按絕对值說都与模 $m_1m_2\cdots\cdots m_k$ 互質。

关于 1 的成立很显然. 因为根据題意, x_1、x_2、……、x_k 分别独立地通过 $\phi(m_1)$、$\phi(m_2)$、……、$\phi(m_k)$ 个数, 而 m_1、m_2、……、m_k 是两两互質的,所以形如(1)的数的个数是:

$$\phi(m_1)\cdot\phi(m_2)\cdot\cdots\cdots\cdot\phi(m_k)=\phi(m_1m_2\cdots\cdots m_k).$$

关于 2 的成立, 可仿照 §5 在討論完全剩余組时, 所举的第五个例題中对应的那部分証明.

关于 3 的成立,我們可以証明:

$$(|M_1x_1+M_2x_2+\cdots\cdots+M_kx_k|,\ m_s)=1.\ (1\leqslant s\leqslant k)$$

如果了解 M_1、M_2、……、M_k 的意义,就可以知道它們中除 M_s 外, 都是 m_s 的倍数,于是得:

$$M_1x_1+M_2x_2+\cdots\cdots+M_kx_k=M_sx_s+m_s\cdot Q.\ (\text{这里 } Q \text{ 是整数})$$

我們知道,如果 $a=bq+c$, 那末$(|a|、|b|)=(|b|、|c|)$.

这样，

$$(|M_1x_1+M_2x_2+\cdots\cdots+M_kx_k|,\ m_s)=(|M_sx_s|,\ m_s).$$

因为 M_s 是 m_1、m_2、……、m_k k 个数中除 m_s 外 $k-1$ 个数的乘积，而且那些数是两两互质的，所以 $(M_s,\ m_s)=1$.

另一方面，x_s 是代表与模 m_s 互質的剩余組内的某一数，当然 $(|x_s|,\ m_s)=1$. 于是可推知：

$$(|M_sx_s|,\ m_s)=1.$$

因此 $(|M_1x_1+M_2x_2+\cdots\cdots+M_kx_k|,\ m_s)=1.$

因为 s 可取 1, 2, ……, k，于是根据互质数的性质可得：

$$(|M_1x_1+M_2x_2+\cdots\cdots+M_kx_k|,\ m_1m_2\cdots\cdots m_k)=1.$$

綜上所述，就証明了：形如(1)的数确实构成了与模 $m_1m_2\cdots\cdots m_k$ 互質的剩余組.

下面我們看一个具体例子：

設 $m_1=6$, $m_2=7$, 当 x_1、x_2 分別独立地通过与 6、7 互質的剩余組时，驗証：形如 $7x_1+6x_2$ 的数构成与模 $6\cdot7$（就是 42）互質的剩余組.

取与模 6 互質的剩余組：1、5；取与模 7 互質的剩余組：1、2、3、4、5、6.

如果 x_1 等于 1，x_2 分別等于 1、2、3、4、5、6 得到的 6 个数是：

13、19、25、31、37、43；

如果 $x_2=5$，x_2分別等于 1、2、3、4、5、6，得到的 6 个数是：

41、47、53、59、65、71；

仔細地观察这 12 个数：13、19、25、31、37、43、41、47、53、59、65、71(其中 43、47、53、59、65、71 这些数，对于模数 42 分別与 1、5、11、17、23、29 同余)，可发現，它們正好构成了与模 42 互質的剩余組.

§8 欧拉定理·費尔馬定理

定理 如果$(|a|,\ m)=1$，那末 $a^{\phi(m)}\equiv1\pmod m$.

（这个定理叫做欧拉定理）

証明 設 m_1、m_2、……、m_k 为与模 m 互质的非負最小剩余組．根据上一节可以知道，与模 m 互质的剩余組含有的数目，有且仅有 $\phi(m)$ 个．所以这里 $k=\phi(m)$．

因为 $(|a|, m)=1$，从上一节定理可知：

$$am_1、am_2、……、am_k \quad (1)$$

也一定是与模 m 互质的剩余組．

又設 r_1、r_2、……、r_k 是分别表示（1）中的数所属的剩余类（以 m 为模）中的非負最小数．

于是，r_1、r_2、……、r_k 也就是与模 m 互质的非負最小剩余組．这样，显然 r_1、r_2、……、r_k 与 m_1、m_2、……、m_k 以全体而言是一致的．也就是，

$$r_1r_2\cdots\cdots r_k=m_1m_2\cdots\cdots m_k.$$

从下面的 k 个同余式：

$am_1\equiv r_1 \pmod m$，$am_2\equiv r_2 \pmod m$，……，$am_k\equiv r_k \pmod m$

可得：$$a^k\cdot m_1m_2\cdots\cdots m_k\equiv r_1r_2\cdots\cdots r_k \pmod m.$$

由上述的 $r_1r_2\cdots\cdots r_k=m_1m_2\cdots\cdots m_k$，且 $(m_1m_2\cdots\cdots m_k, m)=1$（$\because$ m_1、m_2、……、m_k 中每一个都与 m 互质）．从而，上面的同余式变成：$$a^k\equiv 1 \pmod m.$$

因此 $$a^{\phi(m)}\equiv 1 \pmod m.$$

例 判别 49^4-1 能否被 15 整除．

因为 $$\phi(15)=15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=8,$$

而 $49^4=7^8$，且 $(7, 15)=1$，所以 $7^8\equiv 1 \pmod{15}$．

于是 $7^8-1 \vdots 15$．也就是説，$49^4-1 \vdots 15$．

推論 設 p 是质数，如果 $(|a|, p)=1$，那末

$$a^{p-1}\equiv 1 \pmod p.$$

（上面的推論，也叫费尔馬定理）

証明 因为 p 是質数，所以 $\phi(p)=p-1$.

因为 $(|a|, p)=1$, 所以 $a^{p-1}=a^{\phi(p)}\equiv 1 \pmod{p}$.

由費尔馬定理直接可推知：

設 p 是質数，a 是任一整数，那末 $a^p \equiv a \pmod{p}$.

証明

如果 $(|a|, p)=1$, 因为 $a^{p-1}\equiv 1 \pmod{p}$, 可推知：

$$a^p \equiv a \pmod{p}.$$

如果 $(|a|, p)>1$, 因为 p 是質数，所以 $a \vdots p$. 于是 $(a^{p-1}-1)a \vdots p$, 即 $a^p-a \vdots p$, 也就是

$$a^p \equiv a \pmod{p}.$$

例1 試求 47^{7385} 被 17 除后的余数.

因为 7385 被 17—1 除后得：$7385=461\cdot 16+9$, 就是

$$47^{7385}=(47^{16})^{461}\cdot 47^9.$$

根据費尔馬定理，$47^{16}\equiv 1 \pmod{17}$.

但 $47^9\equiv 13^9 \pmod{17}$, 而 $13^2=169\equiv -1 \pmod{17}$, 所以 $13^9=13^8\cdot 13\equiv 13 \pmod{17}$. 也就是說，$47^9\equiv 13 \pmod{17}$.

于是 $$47^{7385}\equiv 47^9\equiv 13 \pmod{17}.$$

例2 設 p 是 2 和 5 以外的任意一个質数，試証：

$$\underbrace{999\cdots\cdots 9}_{(p-1)k\text{ 个}} \vdots p. \quad (k\text{ 是任一个正整数})$$

証明 因为 p 是 2 和 5 以外的質数，那末 $(10, p)=1$. 于是 $(10^k, p)=1$. 根据費尔馬定理，$(10^k)^{p-1}\equiv 1 \pmod{p}$. 也就是說，$10^{k(p-1)}-1 \vdots p$.

很明显，$10^{k(p-1)}-1$ 是一个各位数字都是 9，且位数是 $k(p-1)$ 的数. 因此就証明了論断的成立.

比如： $999999 \vdots 7$; $\underbrace{99\cdots\cdots 9}_{12\text{ 个}} \vdots 13$; 等等.

关于費尔馬定理，是一个值得单独提出的有趣課題. 为了这个目

的，我們介紹两种不需引用前面知識的証法．

先介紹一个証法．証明过程中，应用了"牛頓二項式"公式．

引理 当 p 是質数的时候，$(a+b)^p \equiv a^p+b^p \pmod{p}$．（$a$、$b$ 是任意两个整数）

証明 $(a+b)^p=a^p+C_p^1a^{p-1}b+\cdots\cdots+C_p^{p-1}ab^{p-1}+b^p$． (1)

我們知道：

$$C_p^k=\frac{p(p-1)(p-2)\cdots\cdots(p-k+1)}{1\cdot2\cdot3\cdots\cdots k} \qquad (0<k\leqslant p)$$

是正整数．

当 $k=1$、2、……、$p-1$ 的时候，我們注意数 p 与分母中的任一因数都互質的（因为 p 是質数，且它大于分母中任意一个因数）．于是 $(1\cdot2\cdot3\cdots\cdots k,\ p)=1$．

因此
$$\frac{(p-1)(p-2)\cdots\cdots(p-k+1)}{1\cdot2\cdot3\cdots\cdots k}\text{是正整数．}$$

也就是說，

$$C_p^k=\frac{p(p-1)(p-2)\cdots\cdots(p-k+1)}{1\cdot2\cdot3\cdot\cdots\cdots\cdot k}\ \vdots\ p.$$

$$(k=1、2、\cdots\cdots、p-1)$$

这就表示(1)中除了首末两項以外，其余各項都是 p 的倍数．于是我們可把(1)写作下面的形式：

$$(a+b)^p=a^p+b^p+p\cdot M.\ (M\text{ 是整数})$$

因此
$$(a+b)^p\equiv a^p+b^p \pmod{p}.$$

我們还可以把它推广到：

$$(a_1+a_2+\cdots\cdots+a_n)^p\equiv a_1^p+a_2^p+\cdots\cdots+a_n^p \pmod{p}$$

[这里 p 为質数，a_i（$i=1$、2、……、n）是任意整数.]

証明 当 $n=2$ 时，公式是成立的．

假定 $n=k$ 时，公式也成立，就是

$$(a_1+a_2+\cdots\cdots+a_k)^p\equiv a_1^p+a_2^p+\cdots\cdots+a_k^p \pmod{p}.$$

我們要証明，当 $n=k+1$ 时，公式仍然成立．就是証明：

$$(a_1+a_2+\cdots\cdots+a_k+a_{k+1})^p \equiv a_1^p+a_2^p+\cdots\cdots+a_k^p+a_{k+1}^p \pmod p.$$

設 $a_1+a_2+\cdots\cdots+a_k=A$，根据上面的"引理"得：

$$(A+a_{k+1})^p \equiv A^p+a_{k+1}^p \pmod p.$$

由假定，可知：

$$A^p \equiv a_1^p+a_2^p+\cdots\cdots+a_k^p \pmod p.$$

这样，根据同余的基本性质，就可以推得：

$$A^p+a_{k+1}^p \equiv a_1^p+a_2^p+\cdots\cdots+a_{k+1}^p \pmod p.$$

因此就証明了：

$$(a_1+a_2+\cdots\cdots+a_k+a_{k+1})^p \equiv a_1^p+a_2^p+\cdots\cdots+a_k^p+a_{k+1}^p \pmod p.$$

也就是証明了上面的断言一般地也成立．

由此，立刻可推得費尔馬定理：

如果 p 是質数，而 $(|N|, p)=1$，那末 $N^{p-1}\equiv 1 \pmod p$．

証明

1．如果 $N>0$，在上面的"推广"中，取 $n=N$，且 $a_1=a_2=\cdots\cdots=a_N=1$，那末 $N^p\equiv N \pmod p$．

因为 $(|N|, p)=1$，所以 $N^{p-1}\equiv 1 \pmod p$．[§2 性質 4]

2．如果 $N<0$，設 $N=-N'$ $(N'>0)$．

由 1 可知，$\quad N'^{p-1}\equiv 1 \pmod p$．

于是，$\quad (-N)^{p-1}\equiv 1 \pmod p$．

如果 p 是大于 2 的質数，当然 $p-1$ 必是偶数，因此可推得：

$$N^{p-1}=(-N)^{p-1}\equiv 1 \pmod p.$$

如果 $p=2$，就需証明：$N\equiv 1 \pmod 2$．

事实上，已知 $(|N|, p)=1$，也就是知道了这里的 N 是奇数．显然，上式应該成立．

綜合所述，就証明了費尔馬定理．

下面介紹的費尔馬定理的証明，也不需引用前面的知識，虽然証明的思想方法与上面証明欧拉定理时所用的相类似．

下面我們證明：$a^{p-1}\equiv 1 \pmod p$，p 是質数，且 $(|a|, p)=1$.

證明　設
$$1\cdot a = pq_1 + m_1,\ (0<m_1<p)$$
$$2\cdot a = pq_2 + m_2,\ (0<m_2<p)$$
$$\cdots\cdots\cdots\cdots,$$
$$(p-1)a = pq_{p-1} + m_{p-1}.\ (0<m_{p-1}<p)$$

把上面的一些等式的两边分别相乘，得

$$1\cdot 2\cdot 3\cdot\cdots\cdots\cdot(p-1)\cdot a^{p-1} = \prod_{i=1}^{p-1}(pq_i+m_i)$$
$$= p\cdot M + m_1 m_2\cdots\cdots m_{p-1}.$$

（这里 M 是整数）

于是 $1\cdot 2\cdot 3\cdot\cdots\cdots\cdot(p-1)a^{p-1}\equiv m_1 m_2\cdots\cdots m_{p-1} \pmod p$.　(1)

先来指出 m_1、m_2、……、m_{p-1} 这 $p-1$ 个数，各不相等．如果 $m_s = m_t$ ($s\neq t$，且 $1\leqslant s\leqslant p-1$，$1\leqslant t\leqslant p-1$)，因为 $m_s = sa - pq_s$，$m_t = ta - pq_t$，于是得：　$(s-t)a = p(q_s - q_t)$.

就是　$(s-t)a \vdots p$.

因为 $(|a|, p)=1$，所以 $s-t \vdots p$.

因为 $1\leqslant s\leqslant p-1$，$1\leqslant t\leqslant p-1$，所以要使上式成立，必須 $s=t$. 这就与假定的“$s\neq t$”矛盾了．

因此，$m_s\neq m_t$.

既然 m_1、m_2、……、m_{p-1} 是各不相等，且每一个都是小于 p 的正整数．这样，m_1、m_2、……、m_{p-1} 与 1、2、……、$p-1$ 是全体一致的了．換句話說，

$$m_1 m_2\cdots\cdots m_{p-1} = 1\cdot 2\cdot\cdots\cdots\cdot(p-1).$$

又因为 p 是質数，容易了解 $(1\cdot 2\cdot\cdots\cdots\cdot(p-1), p)=1$. 因此(1)就变成：　$a^{p-1}\equiv 1 \pmod p$.

§9　解同余式的概念

与等式中的情形一样，同余式中存在着絕对同余式——即同余

式对于所含未知数的一切整数值都成立的．例如：$a\equiv a \pmod 5$；$6x^4+9x^3+3x^2+12\equiv 0 \pmod 3$等等．

显然，也存在这样的同余式，它們是永远不成立的．容易举例，如：$5\equiv 3 \pmod 4$；$2x\equiv 1 \pmod 2$等等．

我們感到兴趣的是条件同余式——这种同余式，仅仅对于所含未知数的某一些整数值，才能成立．例如：$x\equiv 2 \pmod 3$；$x^5+x+1\equiv 0 \pmod 7$等等．

根据同余式的性质，可以把同余式右边的一切項都移到左边，所以同余式总可以表示成：

$$f(x)\equiv 0 \pmod m.$$

这里 $f(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n$，$a_i$ 是整数．

（如果整数 a_0 不被 m 整除，那末 n 叫做同余式的次数．）

我們知道，同余式当然也可能含有多个不相同的未知数，不过这里只能对一个未知数的同余式加以討論（即使这样，这里也无法探研过于深奥的問題）．

沒有疑問，解同余式就是要求出适合同余式的未知数的一切整数值（当然，有时它的意义是：指出某一同余式对未知数取任何整数值，都不能成立）．

如同余式

$$f(x)\equiv 0 \pmod m. \tag{1}$$

$f(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n$，$a_i$ 是整数．

我們用模 m 的完全剩余組 0、1、2、……、$m-1$ 分别代入(1)．譬如說，其中的 x_0 满足(1)．也就是說，

$$f(x_0)\equiv 0 \pmod m.$$

我們可以断言：对于模 m 与 x_0 同余的一切数 x 代入(1)也一定适合，也就是满足 $x\equiv x_0 \pmod m$ 的一切 x 值也一定满足(1)［我們把整个 x_0 所属的，以 m 为模的剩余类，算作(1)的一个解］．

根据同余的性质，就可以証明上述断言：

因为 $x\equiv x_0 \pmod{m}$，于是

$$x^n\equiv x_0^n \pmod{m},\ x^{n-1}\equiv x_0^{n-1} \pmod{m},\ \cdots\cdots,\ x\equiv x_0 \pmod{m}.$$

而且

$$a_0x^n\equiv a_0x_0^n \pmod{m},\ a_1x^{n-1}\equiv a_1x_0^{n-1} \pmod{m},\ \cdots\cdots,$$

$$a_{n-1}x\equiv a_{n-1}x_0 \pmod{m}.$$

因此得:

$$a_0x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n$$
$$\equiv a_0x_0^n+a_1x_0^{n-1}+\cdots\cdots+a_{n-1}x_0+a_n \pmod{m}.$$

然而已知: $f(x_0)=a_0x_0^n+a_1x_0^{n-1}+\cdots\cdots+a_n\equiv 0 \pmod{m}$,

因此得: $f(x)=a_0x^n+a_1x^{n-1}+\cdots\cdots+a_n\equiv 0 \pmod{m}$.

例 同余式 $x^5+x+1\equiv 0 \pmod{7}$.

在模 7 的完全剩余組 0、1、2、……、6 中，很容易檢驗出 2、4 适合上式，所以我們説，这同余式有两个解:

$$x\equiv 2 \pmod{7},\quad x\equiv 4 \pmod{7}.$$

当然，这个同余式也只有这两个解.容易想到，如果还有其他的解，这就是説模 7 的完全剩余組内还有其他的数（2、4 以外）也适合同余式，而这是不可能的.

容易了解，如果模 m 的完全剩余組内的所有数分別代入(1)，没有一个是适合的，这就表明(1)无解[不能指望在模 m 的完全剩余組以外的数代入(1)，会恰好适合].

順便提一下解同余式組的概念:

$$\begin{cases} f_1(x)\equiv 0 \pmod{m_1}, \\ f_2(x)\equiv 0 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ f_k(x)\equiv 0 \pmod{m_k}. \end{cases} \tag{2}$$

$f_i(x)$ $(i=1、2、\cdots\cdots、k)$是一个整系数多項式.

所謂解同余式組(2)，意即找出所有适合(2)中每一个同余式的整数值 x.

下面来討論两条定理，从这两条定理可以进一步了解解同余式的概念.

首先应了解两同余式同解的意思：就是指这样的两个同余式，它們的解完全一致（即一个同余式的一切解都适合于另一个同余式；反过来也对）.

定理 同余式

$$f(x)\equiv 0 \pmod p \qquad (1)$$

［这里 $f(x)=a_0x^n+\cdots\cdots+a_n$，$a_i$ 是整数，p 是質数］与一个次数低于 p 的同余式同解.

証明 当然，如果(1)中 $n<p$，就不需要繼續討論了.

如果 $n\geqslant p$，我們用二項式 x^p-x 去除 $f(x)$，即得：

$$f(x)=(x^p-x)\cdot Q(x)+R(x).$$

［这里的整系数多項式 $R(x)$ 次数应小于 p.］

由費尔馬定理知：$x^p-x \vdots p$，于是得

$$f(x)\equiv R(x) \pmod p.$$

所以同余式 $f(x)\equiv 0 \pmod p$ 与 $R(x)\equiv 0 \pmod p$ 是同解的（容易看到，适合前一个同余式的 x 值一定适合后一个同余式；反过来也对）.

例如，同余式

$$f(x)=x^7-2x^5-x^3+x^2+2x-3\equiv 0 \pmod 5.$$

因为 $f(x)=(x^5-x)(x^2-2)+(x^2-3)$，所以原同余式与下面的同余式同解：

$$f'(x)=x^2-3\equiv 0 \pmod 5.$$

我們提出下面的断言：

質数模的 n 次条件同余式，它的解的个数不会超过 n；反过来，如果一个質数模的 n 次同余式具有解的个数多于 n 个，那末这个同余式一定是絕对同余式.

断言眞实性的証明，留給讀者.

这样，以后在討論解質数模的一个未知数的同余式时，就只需研究同余式的次数小于模数的情形就够了.

定理 如果 $m=m_1m_2\cdots\cdots m_k$，且 m_1、m_2、……、m_k 两两互質，那末同余式

$$f(x)\equiv 0 \pmod{m} \tag{2}$$

与同余式組

$$\begin{cases} f(x)\equiv 0 \pmod{m_1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\ f(x)\equiv 0 \pmod{m_k} \end{cases} \tag{3}$$

同解.

[这里同解的意思是：适合(2)的一切整数值 x，一定适合于(3)中的每一个同余式. 反过来，适合同余式組(3)的一切整数值 x，也一定适合(2).]

証明

1. 如果(2)有解，譬如 x_0 是适合(2)的，那末

$$f(x_0)\equiv 0 \pmod{m}.$$

而 m_1、m_2、……、m_k 都是 m 的約数，根据 §1 定理的推論 5 可知，有下列同余式成立：

$$f(x_0)\equiv 0 \pmod{m_1},\ \cdots\cdots,\ f(x_0)\equiv 0 \pmod{m_k}.$$

这就証明了适合(2)的整数值 x 也一定适合于同余式組(3).

2. 如果同余式組(3)有解，譬如 x_0' 是适合同余式組(3)的，那末下列同余式一定成立：

$$f(x_0')\equiv 0 \pmod{m_1},\ \cdots\cdots,\ f(x_0')\equiv 0 \pmod{m_k}.$$

而 m_1、m_2、……、m_k 两两互質，即

$$[m_1,\ m_2,\ \cdots\cdots,\ m_k]=m_1m_2\cdots\cdots m_k=m,$$

由 §2 性質 3 可以推得：

$$f(x_0')\equiv 0 \pmod{m}.$$

这就証明了适合同余式組(3)的一切整数值 x，也一定适合(2).

从以上两个步驟的証明就可以知道(2)与(3)是同解的.

例 同余式 $f(x)\equiv 0 \pmod{30}$ 与同余式組: $f(x)\equiv 0 \pmod{2}$, $f(x)\equiv 0 \pmod{3}$, $f(x)\equiv 0 \pmod{5}$是同解的.

同样的,可以提出下面的断言.关于它的証明留給讀者.

設 T_1、T_2、……、T_k 分別是同余式組(3)中对应的同余式的解的个数,那末同余式(2)的解的个数是 $T=T_1T_2\cdots\cdots T_k$.

关于解同余式的概念,介紹到这里为止.因为这个册子毕竟不是专門探討数論,如果讀者对这个內容有兴趣的話,可以研讀普通的数論課本.那里有着有关这方面的极其丰富的材料.

第六章　整值多項式被某自然数整除問題

这一章所涉及的一些問題,沒有一定的解法可以遵循.我們这里也只能做到这样:按照所依据的定理,把問題分作几种不同的类型,分别地加以解决.

所謂整值多項式就是:对于任何整数 n,如果多項式 $f(n)$ 的值也是整数,那末 $f(n)$ 叫做整值多項式.

§1 借"C_n^r 是整值多項式"解决的問題

定理

$$C_n^r=\frac{n(n-1)(n-2)\cdots\cdots(n-r+1)}{\underline{|r}}$$

是整值多項式.

(这里 r 是正整数, $\underline{|r}=1\cdot 2\cdot 3\cdot\cdots\cdots\cdot r$, n是任意整数)

証明 当 $n\geqslant 0$ 的时候:

如果 $n\geqslant r$, C_n^r 就是从 n 个相异元素中每次不重复地取 r 个元素不同組合个数.显然,这时 C_n^r 是整值.

如果 $0\leqslant n<r$，容易看出：在 n、$n-1$、$n-2$、……、$n-r+1$ 这些数中一定有一个值等于 0，所以这时 $C_n^r=0$. 因此断言也成立.

当 $n<0$ 的时候：

設 $n=-n'$ $(n'>0)$，此时

$$C_n^r=(-1)^r\cdot\frac{n'(n'+1)\cdots\cdots(n'+r-1)}{\underline{|r}}$$

$$=(-1)^r\cdot\frac{(n'+r-1)\cdots\cdots(n'+1)n'}{\underline{|r}}$$

$$=(-1)^rC_{n'+r-1}^r.$$

因为 $n'+r-1>0$，所以 $C_{n'+r-1}^r$ 是整值. 这就推得 C_n^r 也是整值.

定理还可用下面的形式表达：

r 个相邻整数的乘积，一定能被 $\underline{|r}$ 整除.

例如，　$3\cdot4\cdot5\cdot6\ \vdots\ \underline{|4}$；　$11\cdot12\cdot13\cdot14\ \vdots\ \underline{|4}$；

$(-3)\cdot(-2)\cdot(-1)\cdot0\ \vdots\ \underline{|4}$；

$(-15)\cdot(-14)\cdot(-13)\cdot(-12)\ \vdots\ \underline{|4}$.

例 1　求証：整值多项式

$$f(n)=n^3-n\ \vdots\ 6.$$

証明　$f(n)=n(n^2-1)=(n-1)n(n+1)$.

由定理可知，$(n-1)n(n+1)\ \vdots\ \underline{|3}$，而 $\underline{|3}=6$，

所以　$f(n)\ \vdots\ 6$.

例 2　当 n 是奇数时，求証：

$$f(n)=n^2-1\ \vdots\ 8.$$

証明　設 $n=2p+1$（p 是整数），于是

$$f(n)=(2p+1)^2-1=4p\,(p+1).$$

因为 $p(p+1)\ \vdots\ 2$，所以 $f(n)\ \vdots\ 8$.

例 3　求証：整值多项式

$$f(n)=n(n^2+5)\ \vdots\ 6.$$

証明　$f(n)=n[(n^2-1)+6]=n(n^2-1)+6n$.

因为 $n(n^2-1) \vdots 6$，$6n \vdots 6$，所以 $f(n) \vdots 6$.

例 4 求証：三个相邻整数的立方和能被 9 整除.

証明 設三个相邻整数是：$n-1$、n、$n+1$.

容易看出：$(n-1)^3+n^3+(n+1)^3=3n(n^2+2)$.

而 $n(n^2+2)=n[(n^2-1)+3]=n(n^2-1)+3n \vdots 3$,

所以 $$(n-1)^3+n^3+(n+1)^3 \vdots 9.$$

例 5 如果 p 是一个正奇数，求証：整値多項式
$$f(n)=n^p-n \vdots 6.$$

証明 $f(n)=n(n^{p-1}-1)$，这里 $p-1$ 是偶数，設 $p-1=2t$，于是
$$f(n)=n(n^{2t}-1)$$
$$=n(n^2-1)[n^{2(t-1)}+n^{2(t-2)}+\cdots\cdots+1] \vdots 6.$$

例 6 如果 n 是偶数，求証：
$$f(n)=n^3+20n \vdots 48;$$
$$f_1(n)=n^3-4n \vdots 48.$$

証明 設 $n=2p$，于是
$$f(n)=n(n^2+20)=2p(4p^2+20)=8p(p^2+5).$$

已知 $p(p^2+5) \vdots 6$，所以 $f(n) \vdots 48$.
$$f_1(n)=n(n^2-4)=2p(4p^2-4)=8p(p^2-1).$$

已知 $p(p^2-1) \vdots 6$，所以 $f_1(n) \vdots 48$.

例 7 求証：整値多項式
$$f(n)=n(n+1)(2n+1) \vdots 6.$$

証明
$$f(n)=n(n+1)[(n-1)+(n+2)]$$
$$=(n-1)n(n+1)+n(n+1)(n+2).$$

而 $(n-1)n(n+1)$ 与 $n(n+1)(n+2)$ 都能被 6 整除，所以 $f(n) \vdots 6$.

例 8 求証：整値多項式
$$f(n)=n^2(n^2-1) \vdots 12.$$

的 **証明** 我們只需証明 $f(n) \vdots 3$，又 $f(n) \vdots 4$.

因为$f(n)=(n-1)n(n+1)n$，而$(n-1)n(n+1)\vdots 6$，所以$f(n)\vdots 3$.

此外，如果n是偶数，当然$n^2\vdots 4$. 就是説，$f(n)\vdots 4$.

如果n是奇数，当然$n^2-1=(n+1)(n-1)\vdots 4$. 也就是説，$f(n)\vdots 4$.

綜上所述，就証明了 $f(n)\vdots 12$.

例 9 求証：

整值多項式 $f(n)=n(n+2)(5n+1)(5n-1)\vdots 24$.

証明

因为
$$\begin{aligned} f(n)&=n(n+2)(25n^2-1)\\ &=n(n+2)[(n^2-1)+24n^2]\\ &=(n-1)n(n+1)(n+2)+24n^3(n+2), \end{aligned}$$
而$(n-1)n(n+1)(n+2)\vdots \underline{|4}$，所以$f(n)\vdots 24$.

例 10 求証：

整值多項式 $f(n)=n^5-5n^3+4n\vdots 120$.

証明

因为
$$\begin{aligned} f(n)&=n(n^4-5n^2+4)\\ &=n(n^2-1)(n^2-4)\\ &=(n-2)(n-1)n(n+1)(n+2), \end{aligned}$$
而$(n-2)(n-1)n(n+1)(n+2)\vdots \underline{|5}$，所以$f(n)\vdots 120$.

例 11 求証：

整值多項式 $f(n)=n^2(2n^4+3n^3-n^2-3n-1)\vdots 36$.

証明

因为
$$\begin{aligned} f(n)&=n^2[2n^2(n^2-1)+3n(n^2-1)+(n^2-1)]\\ &=n^2(n^2-1)(2n^2+3n+1)\\ &=n^2(n^2-1)(2n+1)(n+1)\\ &=[(n-1)n(n+1)][n(n+1)(2n+1)], \end{aligned}$$
而$(n-1)n(n+1)\vdots 6$，又$n(n+1)(2n+1)\vdots 6$，所以$f(n)\vdots 36$.

例 12 求証：

$$f(n)=\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$$

是整值多項式.

証明
$$f(n)=\frac{1}{6}(2n^3+3n^2+n)$$
$$=\frac{1}{6}n(n+1)(2n+1).$$

如果 n 取整数，显然，$n(n+1)(2n+1)\vdots 6$，所以 $f(n)$ 为整值多項式.

例 13 求証:

$$f(n)=n(n-1)(n-2)\frac{3n-5}{12}$$

是整值多項式.

証明 因为 $\frac{3n-5}{12}=\frac{1}{3}+\frac{n-3}{4}$,

所以 $f(n)=\frac{n(n-1)(n-2)}{3}+\frac{n(n-1)(n-2)(n-3)}{4}$.

如果 n 取整数，显然，$n(n-1)(n-2)\vdots 3$，以及

$n(n-1)(n-2)(n-3)\vdots 4$. 因此 $f(n)$ 是整值多項式.

例 14 求証:

$$f(n)=\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n$$

是整值多項式.

証明

$$f(n)=\frac{1}{15}(3n^5+5n^3+7n)$$
$$=\frac{1}{15}[3(n^5-5n^3+4n)+20n^3-5n]$$
$$=\frac{1}{15}[3(n-2)(n-1)n(n+1)(n+2)$$
$$+20(n-1)n(n+1)+15n].$$

显然，括号内的每一項都能被 15 整除．所以 $f(n)$ 确是一个整值多項式．

值得指出，这种类型的問題，用数学归納法都可获得証明（虽然对某些問題来說，应用数学归納法可能会感到繁杂）．現在我們从上面选取几个問題，用数学归納法証明于后．

例 1 用数学归納法証明：

三相邻整数的立方和能被 9 整除．

証明 設三相邻整数是 $n-1$、n、$n+1$，就是求証：

$$f(n)=(n-1)^3+n^3+(n+1)^3 \vdots 9.$$

1．当 $n \geqslant 0$ 的时候：

(1) 如果 $n=0$，显然，$f(0)=0 \vdots 9$．

(2) 設 $n=k$ 时，这个断言成立．就是

$$f(k)=(k-1)^3+k^3+(k+1)^3 \vdots 9.$$

我們証明：$f(k+1) \vdots 9$．

$$\begin{aligned} f(k+1) &= k^3+(k+1)^3+(k+2)^3 \\ &= k^3+(k+1)^3+k^3+6k^2+12k+8 \\ &= [(k-1)^3+k^3+(k+1)^3]+(9k^2+9k+9). \end{aligned}$$

显然，等号右边的两部分都能被 9 整除，所以 $f(k+1) \vdots 9$．

这样我們証明了，当 $n \geqslant 0$ 时，$f(n) \vdots 9$．

2．当 $n<0$ 的时候：設 $n=-n'(n'>0)$，

$$\begin{aligned} f(n) &= (n-1)^3+n^3+(n+1)^3 \\ &= -[(n'+1)^3+n'^3+(n'-1)^3]. \end{aligned}$$

因为 $n'>0$，当然 $(n'+1)^3+n'^3+(n'-1)^3 \vdots 9$．因此 $f(n) \vdots 9$．

綜上所述，就証明了：对于任意整数 n，一定有

$$f(n) \vdots 9.$$

例 2 用数学归納法証明：

整值多项式 $f(n)=n(n+1)(2n+1) \vdots 6$．

証明 1．当 $n \geqslant 0$ 的时候：

(1) 如果 $n=0$，显然，$f(0)=0 \vdots 6$。

(2) 設 $n=k$ 时，$f(k)=k(k+1)(2k+1) \vdots 6$.

我們証明：$f(k+1) \vdots 6$.

因为 $f(k+1)-f(k)=(k+1)(k+2)(2k+3)-k(k+1)(2k+1)$

$$=(k+1)[(k+2)(2k+3)-k(2k+1)]$$

$$=6(k+1)^2 \vdots 6.$$

又因为假定 $f(k) \vdots 6$，所以 $f(k+1) \vdots 6$.

上面証明了，当 $n\geqslant 0$ 时，$f(n) \vdots 6$.

2. 当 $n<0$ 的时候：設 $n=-n'(n'>0)$，那末

$$f(n)=n(n+1)(2n+1)$$

$$=-n'(n'-1)(2n'-1).$$

我們就需証明：对于正整数 n'，

$$f_1(n')=n'(n'-1)(2n'-1) \vdots 6.$$

設 $n'=m+1$（当然 m 是非負整数）.

显然，$f_1(n')=(m+1)m(2m+1)$. 由 1 可知，$f_1(n') \vdots 6$.

上面也就証明了，当 $n<0$ 时，$f(n) \vdots 6$.

綜上所述，証明了整值多項式 $f(n) \vdots 6$.

例 3 用数学归納法証明：

$$f(n)=\frac{1}{5}n^5+\frac{1}{3}n^3+\frac{7}{15}n$$

是整值多項式.

証明 1. 当 $n\geqslant 0$ 的时候：

(1) 如果 $n=0$，显然，$f(0)=0$. 就是說，这时断言是成立的.

(2) 設 $f(k)=\frac{1}{5}k^5+\frac{1}{3}k^3+\frac{7}{15}k$ 是整值多項式. 也就是說，

$$f_1(k)=15f(k)=3k^5+5k^3+7k \vdots 15.$$

我們証明：$f(k+1)$ 也是整值多項式. 也就需証明

$$f_1(k+1)=15f(k+1) \vdots 15.$$

因为

$$f_1(k+1)=3(k+1)^5+5(k+1)^3+7(k+1)$$
$$=k(3k^4+5k^2+7)+(15k^4+30k^3+45k^2+30k+15).$$

而 $k(3k^4+5k^2+7) \vdots 15$，显然，

$$15k^4+30k^3+45k^2+30k+15 \vdots 15.$$

因此 $f_1(k+1) \vdots 15$. 于是就証明了：当 $n \geqslant 0$ 时，$f(n)$是整值多項式.

2. 当 $n<0$ 的时候：設 $n=-n'$ $(n'>0)$.

于是
$$f(n)=-\left(\frac{1}{5}n'^5+\frac{1}{3}n'^3+\frac{7}{15}n'\right).$$

因为 $n'>0$，当然$\frac{1}{5}n'^5+\frac{1}{3}n'^3+\frac{7}{15}n'$是整值多項式. 因此当$n<0$时，$f(n)$也是整值多項式.

下面我們选出几个問題，供讀者練习.

1. 求証：r 个相邻偶数的乘积能被 $2^r|\underline{r}$ 整除.
2. 求証：对于任意整数 n，$n^2 \pm n$ 一定是偶数.
3. 求証：整值多項式 $f(n)=n(n^2+2) \vdots 3$.
4. 求証：整值多項式 $f(n)=n(2n+1)(7n+1) \vdots 6$.
5. 求証：如果 n 是奇数，$f(n)=n^5-n \vdots 12$.
6. 求証：整值多項式 $f(n)=n(n^2-1)(3n+2) \vdots 24$.
7. 求証：整值多項式 $f(n)=n(n^2-49)(n^2+49) \vdots 30$.

§2 借費尔馬定理解决的問題

例1 求証：整值多項式 $f(n)=n^7-n \vdots 42$.

証明 首先，明显地有 $f(n) \vdots 7$（費尔馬定理）. 又因为

$$f(n)=n(n^6-1)$$
$$=n(n^2-1)(n^4+n^2+1) \vdots 6,$$

因此 $f(n) \vdots 42$.

例 2 設 $|n|$ 是大于 3，且不等于 7 的質数，求証：

$$f(n)=n^6-1 \vdots 168.$$

証明 因为 $168=8\cdot3\cdot7$，而 8、3、7 是两两互質的数．所以只需証明 $f(n)$ 分别能被 3、7、8 整除．

首先，根据費尔馬定理，$f(n) \vdots 7$。

其次，因为 $f(n) \vdots n^2-1$，而根据費尔馬定理，$n^2-1 \vdots 3$，因此 $f(n) \vdots 3$.

另一方面，由条件可知，这里 n 是奇数，所以 $n^2-1 \vdots 8$（参閱 §1 例 2）．也就是 $f(n) \vdots 8$.

綜上所述，即証明了 $f(n) \vdots 168$.

注 事实上，可以把条件放寬，变成：$(|n|, 168)=1$.

例 3 求証：整値多項式 $f(n)=n^{13}-n \vdots 5460$.

証明 $5460=13\cdot7\cdot4\cdot3\cdot5$.

（13、7、4、3、5 是两两互質的）

容易看出，$f(n)=n^{13}-n$，$f_1(n)=n^7-n$，$f_2(n)=n^4-n$，

$f_3(n)=n^3-n$，$f_4(n)=n^5-n$ 都是 $f(n)$ 的因数．

由費尔馬定理知：$f(n) \vdots 13$，$f_1(n) \vdots 7$，$f_2(n) \vdots 4$，$f_3(n) \vdots 3$，$f_4(n) \vdots 5$．就是 $f(n)$ 能被 13、7、4、3 及 5 整除，所以 $f(n) \vdots 5460$.

例 4 設 p 是大于 3 的質数，求証：

整値多項式 $f(n)=n^p-n \vdots 6p$.

証明 首先，由費尔馬定理知，$f(n) \vdots p$.

另一方面，我們知道 $f(n) \vdots 6$（参閱 §1 例 5）．

无疑的，这里 $(p, 6)=1$，因此証得：$f(n) \vdots 6p$.

例 5 設 m 是質数，正整数 a、b 都小于 m，求証：

$$a^{m-2}+a^{m-3}b+\cdots\cdots+ab^{m-3}+b^{m-2} \vdots m.$$

証明 因为 m 分别与 a 及 b 都互質，由費尔馬定理可知：

$$a^{m-1}-1 \vdots m, \quad b^{m-1}-1 \vdots m.$$

所以 $\quad a^{m-1}-b^{m-1}=(a^{m-1}-1)-(b^{m-1}-1) \vdots m.$

也就是說，$(a-b)(a^{m-2}+a^{m-3}b+\cdots\cdots+ab^{m-3}+b^{m-2}) \vdots m$.

观察条件，可知 $|a-b|$ 与 m 是互質的.

因此，　$a^{m-2}+a^{m-3}b+\cdots\cdots+ab^{m-3}+b^{m-2} \vdots m$.

注　事实上，可以把条件放寬，变成：

非零整数 a、b 与質数 m 間有下列关系：

$$(|a|, m)=1, \quad (|b|, m)=1; \quad (|a-b|, m)=1.$$

例 6　設 p 是質数，$(|n|, p)=1$，且 r 是任意正整数，求証：

$$n^{p^r-p^{r-1}}-1 \vdots p^r.$$

証明　由費尔馬定理可知：$n^{p-1}-1 \vdots p$，也就是，$n^{p-1}=1+pN$.（N 是整数）

因此，

$$(n^{p-1})^{p^{r-1}}=(1+pN)^{p^{r-1}}$$
$$=1+p^rM.（M 是整数）$$

［因为二項式 $(1+pN)^{p^{r-1}}$ 展开式中，从第二項起所有的項都能被 p^r 整除.］

这就証明了

$$n^{p^r-p^{r-1}}-1 \vdots p^r.$$

例 7　如果 $a^2+b^2=c^2$（a、b、c 是整数），求証：$abc \vdots 60$.

証明　由已知条件可推出：

$$|a|=m^2-n^2, \quad |b|=2mn, \quad |c|=m^2+n^2.$$

（m、n 是正整数，且 $m \geqslant n$）

反过来，也可由此推出　$a^2+b^2=c^2$.

于是就只需証明：$2mn(m^2-n^2)(m^2+n^2) \vdots 60$. 也就是只需証明：

$$mn(m^2-n^2)(m^2+n^2) \vdots 30.$$

首先可断言 $mn(m^2-n^2)(m^2+n^2) \vdots 2$.

如果 m、n 中有一个是偶数，断言就成立. 如果 m、n 两个都是奇数，显然，m^2+n^2（m^2-n^2 也一样）就是偶数，因此断言也成立.

而 $(2, 15)=1$，这样就只需証明：

$$mn(m^2-n^2)(m^2+n^2) \vdots 15.$$

也就是只要証明以下两个方面：

(1) 求証：$mn(m^2-n^2)(m^2+n^2) \vdots 3$.

观察 $mn(m^2-n^2)=mn[(m^2-1)-(n^2-1)]$

$$=n(m^3-m)-m(n^3-n),$$

由費尔馬定理知：$m^3-m \vdots 3$, $n^3-n \vdots 3$.

因此 $mn(m^2-n^2) \vdots 3$. 也就是說，$mn(m^2-n^2)(m^2+n^2) \vdots 3$.

(2) 求証：$mn(m^2-n^2)(m^2+n^2) \vdots 5$.

观察 $mn(m^2-n^2)(m^2+n^2)=mn(m^4-n^4)$

$$=n(m^5-m)-m(n^5-n),$$

因为 $m^5-m \vdots 5$, $n^5-n \vdots 5$, 所以

$$mn(m^2-n^2)(m^2+n^2) \vdots 5.$$

因此 $$mn(m^2-n^2)(m^2+n^2) \vdots 15.$$

綜上所述，即証明了 $abc \vdots 60$.

下面几个問題，留給讀者練习.

1. 求証：整值多項式 $f(n)=n^5-n \vdots 30$.
2. 求証：整值多項式 $f(n)=n^9-n^3 \vdots 42$.
3. 設$|a|$、$|b|$是大于5的質数，求証：$a^4-b^4 \vdots 120$.
4. 設$|a|$、$|b|$都与5460互質，求証：$a^{12}-b^{12} \vdots 5460$.
5. 設 a、b 是任意两个整数，求証：$ab(a^3+b^3)(a^3-b^3) \vdots 28$.

§3 借定理“$a^n-b^n \vdots a-b$”解决的問題

定理 a、b 是整数，对于任意的正整数 n，有

$$a^n-b^n \vdots a-b,$$

且 $$\frac{a^n-b^n}{a-b}=a^{n-1}+a^{n-2}b+\cdots\cdots+ab^{n-2}+b^{n-1}.$$

（这个定理在中学代数課本中已介紹过，这里就引用了.）

推論 1. 对于任意的正偶数 n，有

$$a^n-b^n \vdots a+b,$$

且
$$\frac{a^n-b^n}{a+b}=a^{n-1}-a^{n-2}b+\cdots\cdots+(-1)^{n-1}b^{n-1}.$$

2. 对于任意的正奇数 n，有

$$a^n+b^n \vdots a+b,$$

且
$$\frac{a^n+b^n}{a+b}=a^{n-1}-a^{n-2}b+\cdots\cdots+(-1)^{n-1}b^{m-1}.$$

例如，$f(n)=2^{4n}-1 \vdots 2^4-1$.

又如，可断言 7^4-16 能被5整除，也能被9整除（因 $7^4-16=7^4-2^4$）.

例1 如果 n 是非負整数，求証：

$$f(n)=3^{4n+2}+5^{2n+1} \vdots 14.$$

証明 因为 $f(n)=9^{2n+1}+5^{2n+1}$，由推論2知：$f(n) \vdots 9+5$. 也就是說，$f(n) \vdots 14$.

例2 如果 n 是非負整数，求証：

$$f(n)=8^{n+2}+9^{2n+1} \vdots 73.$$

証明 因为
$$\begin{aligned}f(n)&=64\cdot8^n+9\cdot81^n\\&=73\cdot8^n-9\cdot8^n+9\cdot81^n\\&=73\cdot8^n+9(81^n-8^n),\end{aligned}$$

而 $81^n-8^n \vdots 81-8$，也就是 $81^n-8^n \vdots 73$，所以 $f(n) \vdots 73$.

例3 如果 n 是非負整数，求証：

$$f(n)=2^{12n+9}-5^{4n+1} \vdots 39.$$

証明

因为 $f(n)=8^{4n+3}-5^{4n+1}=512\cdot8^{4n}-5\cdot5^{4n}$,

又 $512=13\cdot39+5$，所以

$$\begin{aligned}f(n)&=13\cdot39\cdot8^{4n}+5\cdot8^{4n}-5\cdot5^{4n}\\&=13\cdot39\cdot8^{4n}+5(8^{4n}-5^{4n}).\end{aligned}$$

显然，$8^{4n}-5^{4n}=64^{2n}-25^{2n} \vdots 64-25$，所以 $f(n) \vdots 39$.

例 4 如果 n 是非负整数，a 是任意整数，求証：

$$f(n)=a^{n+2}+(a+1)^{2n+1} \vdots a^2+a+1.$$

証明 因为 $f(n)$

$$\begin{aligned}
&=a^2\cdot a^n+(a+1)\cdot(a+1)^{2n}\\
&=a^2\cdot a^n+(a+1)(a^2+2a+1)^n\\
&=(a+1)(a^2+2a+1)^n+a^2(a^2+2a+1)^n\\
&\quad -a^2(a^2+2a+1)^n+a^2\cdot a^n\\
&=(a^2+a+1)(a^2+2a+1)^n-a^2[(a^2+2a+1)^n-a^n].
\end{aligned}$$

显然，$(a^2+2a+1)^n-a^n \vdots a^2+a+1$. 因此

$$f(n) \vdots a^2+a+1.$$

注 例 2 就是这个例子的特殊情况.

例 5 如果 n 是非负整数，求証：

$$f(n)=3\cdot 5^{2n+1}+2^{3n+1} \vdots 17.$$

証明 因为 $f(n)=15\cdot 25^n+2\cdot 8^n$

$$\begin{aligned}
&=17\cdot 25^n-2\cdot 25^n+2\cdot 8^n\\
&=17\cdot 25^n-2[25^n-8^n],
\end{aligned}$$

显然，$25^n-8^n \vdots 17$. 因此 $f(n) \vdots 17$.

例 6 如果 n 是非负整数，求証：

$$f(n)=5^{2n+1}+2^{n+4}+2^{n+1} \vdots 23.$$

証明 因为 $f(n)=5^{2n+1}+18\cdot 2^n$

$$\begin{aligned}
&=5\cdot 25^n+18\cdot 2^n\\
&=23\cdot 25^n-18(25^n-2^n),
\end{aligned}$$

显然，$25^n-2^n \vdots 23$, 因此 $f(n) \vdots 23$.

例 7 如果 n 是非负整数，求証：

$$f(n)=2^{6n+10}+2^{6n+6}+3^2\cdot 2^{6n+5}+2^7\cdot 3^{2n+1}+2^3\cdot 3^{2n+1}$$
$$+2^2\cdot 3^{2n+3} \vdots 1892.$$

証明 因为 $1892=2^2\cdot 11\cdot 43$, 設 $f(n)=2^2\cdot f_1(n)$, 于是只需証明：

$$f_1(n)=2^{6n+8}+2^{6n+4}+3^2\cdot 2^{6n+3}+2^5\cdot 3^{2n+1}+2\cdot 3^{2n+1}$$

$$+3^{2n+3} \vdots 11\cdot 43.$$

事实上，$f_1(n)=(2^5+2+3^2)2^{6n+3}+(2^5+2+3^2)3^{2n+1}$

$$=43(2^{6n+3}+3^{2n+1})$$

$$=43(8^{2n+1}+3^{2n+1}) \vdots 43\cdot 11.$$

例 8 如果 n 是正整数，求証：

$$f(n)=6^{10n+1}+5^{11n-1} \vdots 31.$$

証明 因为 5^{10n+1} 与 31 互质，所以只需証明：

$$f_1(n)=5^{10n+1}\cdot f(n)=30^{10n+1}+5^{21n} \vdots 31.$$

因为 $f_1(n)=30\cdot 30^{10n}+5^{21n}$

$$=31\cdot 30^{10n}-[(30^{10})^n-(5^{21})^n],$$

这样就需証明：$(30^{10})^n-(5^{21})^n \vdots 31$. 因此也就只需証明：

$$30^{10}-5^{21} \vdots 31.$$

因为 $30\equiv -1 \pmod{31}$，所以 $30^{10}\equiv 1 \pmod{31}$；

因为 $5^3=125\equiv 1 \pmod{31}$，所以 $5^{21}\equiv 1 \pmod{31}$.

于是 $30^{10}-5^{21}\equiv 0 \pmod{31}$. 也就是說，$30^{10}-5^{21} \vdots 31$.

事实上，根据同余的性质，立刻可以証明：$f_1(n) \vdots 31$.

因为 $30\equiv -1 \pmod{31}$，而 $10n+1$ 是一个奇数，所以

$$30^{10n+1}\equiv -1 \pmod{31}.$$

因为 $5^3\equiv 1 \pmod{31}$，所以 $5^{21n}\equiv 1 \pmod{31}$. 于是 $30^{10n+1}+5^{21n}\equiv 0 \pmod{31}$. 就是說，$f_1(n) \vdots 31$.

例 9 如果 n 是非負整数，求証：

$$f(n)=2^{3n+3}-7n+41 \vdots 49.$$

証明 因为 $f(n)=(8^{n+1}-7n-8)+49$，而

$$8^{n+1}-7n-8=(8^{n+1}-1)-(n+1)\cdot 7$$

$$=(8-1)(8^n+8^{n-1}+\cdots\cdots+8+1)-(n+1)\cdot 7$$

$$=7(8^n+8^{n-1}+\cdots\cdots+8+1-1-n)$$

$$=7[(8^n-1)+(8^{n-1}-1)+\cdots\cdots+(8-1)].$$

显然，$(8^n-1)+(8^{n-1}-1)+\cdots\cdots+(8-1) \vdots 7$.

因此 $8^{n+1}-7n-8 \vdots 49$. 也就是 $f(n) \vdots 49$.

上面这种类型的题目，大多可用数学归納法加以証明的. 兹举几个例子于后.

例 1 用数学归納法証明：

如果 n 是非負整数，那末 $f(n)=8^{n+2}+9^{2n+1} \vdots 73$.

証明

1. 当 $n=0$ 时，显然，$f(0)=8^2+9=73 \vdots 73$.

2. 設 $f(k) \vdots 73$，証明：$f(k+1) \vdots 73$.

因为
$$\begin{aligned} f(k+1) &= 8^{k+3}+9^{2k+3} \\ &= 8\cdot 8^{k+2}+81\cdot 9^{2k+1} \\ &= 8(8^{k+2}+9^{2k+1})+73\cdot 9^{2k+1} \\ &= 8\cdot f(k)+73\cdot 9^{2k+1}, \end{aligned}$$

由假設 $f(k) \vdots 73$，因此 $f(k+1) \vdots 73$.

綜上所述，就証明了：如果 n 是非負整数，那末 $f(n) \vdots 73$.

例 2 用数学归納法証明：

如果 n 是非負整数，那末

$$f(n)=a^{n+2}+(a+1)^{2n+1} \vdots a^2+a+1.$$

証明

1. 当 $n=0$ 时，显然，$f(0)=a^2+a+1 \vdots a^2+a+1$.

2. 設 $f(k) \vdots a^2+a+1$，証明：$f(k+1) \vdots a^2+a+1$.

因为
$$\begin{aligned} f(k+1) &= a^{k+3}+(a+1)^{2k+3} \\ &= a\cdot a^{k+2}+(a+1)^2\cdot(a+1)^{2k+1} \\ &= a\cdot a^{k+2}+(a^2+a+1)(a+1)^{2k+1}+a(a+1)^{2k+1} \\ &= a[a^{k+2}+(a+1)^{2k+1}]+(a^2+a+1)(a+1)^{2k+1} \\ &= a\cdot f(k)+(a^2+a+1)(a+1)^{2k+1}, \end{aligned}$$

由假設 $f(k) \vdots a^2+a+1$，因此 $f(k+1) \vdots a^2+a+1$.

綜上所述，就証明了：如果 n 是非負整数，那末 $f(n) \vdots a^2+a+1$.

例 3 用数学归納法証明：

如果 n 是非負整数，那末

$$f(n)=2^{3n+3}-7n+41 \vdots 49.$$

証明

1. 当 $n=0$ 时，$f(0)=2^3+41 \vdots 49$.

2. 設 $f(k) \vdots 49$，証明：$f(k+1) \vdots 49$.

因为 $f(k+1)=2^{3k+6}-7(k+1)+41$

$$=8\cdot 2^{3k+3}-7k+41-7$$

$$=(2^{3k+3}-7k+41)+7(2^{3k+3}-1)$$

$$=f(k)+7(8^{k+1}-1),$$

由假設 $f(k) \vdots 49$，而 $7(8^{k+1}-1) \vdots 7\cdot 7$，因此 $f(k+1) \vdots 49$.

綜上所述，就証明了，如果 n 是非負整数，那末 $f(n) \vdots 49$.

下面几个問題，留給讀者練习.

1. 設 n 是非負整数，求証：

$$f(n)=n(n+1)(3^{2n+1}+1) \vdots 8.$$

2. 設 n 是非負整数，求証：

$$f(n)=3^{n+2}+4^{2n+1} \vdots 13.$$

3. 設 n 是非負整数，求証：

$$f(n)=11^{n+2}+12^{2n+1} \vdots 133.$$

4. 設 n 是非負整数，求証：

$$f(n)=2^{12n+2}+3^{3n+2} \vdots 13.$$

5. 設 n 是非負整数，求証：

$$f(n)=3^{2n+2}-8n-9 \vdots 64.$$

6. 設 n 是非負整数，求証：

$$f(n)=3^{2n+1}+40n-67 \vdots 64.$$

7. 設 n 是非負整数，求証：

$$f(n)=7^{2n+1}-48n-7 \vdots 288.$$

8. 設 n 是非負整数，求証：

$$f(n)=3^{2n+5}+160n^2-56n-243 \vdots 512.$$

第七章 不定方程

所謂不定方程,是指的未知数的个数多于方程个数的那些方程.例如,方程

$$ax+by=c,$$

$$ax+by+cz=d,$$

$$x^2+y^2=z^2,$$

$$ax^2+bxy+cy^2+dx+ey+f=0$$

等等.

研究整系数不定方程的整数解,是数論中的丰富且有趣的問題之一.另一方面,关于不定方程的討論是异常的繁瑣与复杂,甚至有着不少极其困难的問題.基于这个册子的性质,只可能介紹一些簡单的情形:整系数二元一次方程的整数解;最簡单的三元二次方程的整数解;以及粗略地提及一些費尔馬大定理的知識.

§1 整系数两元一次方程的整数解

1. 整系数方程 $ax+by=c$ 存在整数解的充分而且必要条件

定理 設 $a(\neq 0)$、$b(\neq 0)$、c 是整数,那末

$$ax+by=c \tag{I}$$

存在整数解的充分而且必要条件是:

$$c \vdots d. \quad [这里\ d=(|a|;\ |b|)]$$

証明 关于条件的必要性:

如果(I)具有整数解 x_0, y_0, 又設

$$a=dq_1,\ b=dq_2,\ [显然,\ (|q_1|,\ |q_2|)=1]$$

于是 $$d(q_1x_0+q_2y_0)=c.$$

因此推得: $$c \vdots d.$$

至于条件的充分性,因为在下一章中会有交代,这里就先承認了它

的正确性.

例如,可以断言方程 $4x+6y=7$ 沒有整数解.

因为 $(4, 6)=2$, 而 7 不能被 2 整除.

又如,可以断言方程 $2x+3y=4$ 一定有整数解.

推論 方程 $ax+by=d$ $[d=(|a|, |b|)]$ 一定有整数解.

特殊情形: 如果 $(|a|, |b|)=1$, 那末 $ax+by=1$ 一定有整数解.

这个"特殊情形", 容易指出它的价值(在某些書上, 多有以它为基础,来推导出諸如第一章中的一些定理):

例如,定理"对于正整数 a、b、c, 如果 $ac \vdots b$, 且 $(a, b)=1$, 那末 $c \vdots b$." 可証明如下:

对于互質的两正整数 a、b,已知一定存在整数 x、y,使 $ax+by=1$。以 c 乘方程的两边得:

$$acx+bcy=c.$$

在这个方程中,左边的两項都能被 b 整除,所以 $c \vdots b$.

又如,定理"如果 a、c 都与 b 互質,那末 $(ac, b)=1$." 可証明如下:

对于互質的 a、b, 一定存在整数 x、y, 使

$$ax+by=1.$$

于是

$$acx+bcy=c.$$

如果 $(ac, b)=d>1$, 由上式,就得到 $c \vdots d$. 这样,由 "$b \vdots d$, $c \vdots d$" 就得到 $(b, c)>1$. 显然,这与已知条件是矛盾的.因此

$$(ac, b)=1.$$

2. 整系数方程 $ax+by=c$ 整数解的公式

如果整系数方程 $ax+by=c$ 具有整数解,当然應有 $c \vdots (|a|, |b|)$. 因此这里研究 $ax+by=c$ 的整数解問題,不妨首先假定 $(|a|, |b|)=1$.

設 x_0、y_0 是整系数方程

$$ax+by=c \quad [(|a|, |b|)=1] \tag{I}$$

的某一組整数解.于是

$$ax_0+by_0=c.$$

这样，可得：　　$a(x-x_0)+b(y-y_0)=0$.

也就是

$$y=y_0+\frac{a(x_0-x)}{b}.$$

由整数值 x，要得到整数值 y，应使

$$a(x_0-x) \vdots b.$$

而$(|a|, |b|)=1$，所以只需使：$x_0-x \vdots b$.

設 $x_0-x=bt$ (t 是整数)，于是得：

$$x=x_0-bt, \quad y=y_0+at. \qquad \text{(II)}$$
$$(t=0、\pm1、\pm2、\cdots\cdots)$$

这說明如果方程 (I) 有一組整数解 x_0、y_0，那末它的一切整数解可由关系式(II)求得.

这个事实，可以檢驗如下：

設 $t=t_1$，得到一組值 x_1、y_1. 也就是

$$x_1=x_0-bt_1, \quad y_1=y_0+at_1.$$

可以驗証，这組解是一定适合方程(I)的.

事实上，
$$\begin{aligned} &ax_1+by_1 \\ &=a(x_0-bt_1)+b(y_0+at_1) \\ &=ax_0+by_0. \end{aligned}$$

已知 $ax_0+by_0=c$，因此 $ax_1+by_1=c$.

3. 方程 $ax+by=c$ 一組特殊的整数解的求法

我們已經知道，求 $ax+by=c$ 的一切整数解的問題，归結成只需要求出它的一組特殊的整数解. 这是个不很困难的問題，玆举几个例于后.

例 1　求方程 $7x-4y=2$ 的整数解.

以 x 表示系数較小的 y，得

$$y=\frac{7x-2}{4}.$$

我們观察上式，当 x 取什么整数值时，使对应的 y 得到整数值.

很清楚，当 $x=2$ 时，$7x-2 \vdots 4$.

也就是說，
$$y=\frac{1}{4}(7\cdot 2-2)=3.$$

于是，方程的一組特殊的整数解求得. 由上节可知，方程的一切整数解，可由下面的公式給出：

$$x=2+4t, \quad y=3+7t. \ (t \text{ 是整数})$$

例 2 求方程 $7x+19y=213$ 的整数解.

以 y 表示系数較小的 x，得：

$$x=\frac{213-19y}{7}.$$

将上式分出整式，就得到：

$$x=30-2y+\frac{3-5y}{7}.$$

因此，当 y 是整数的时候，要使对应的 x 也是整数，就必須 $\frac{1}{7}(3-5y)$ 是整数.

今設
$$\frac{1}{7}(3-5y)=m \ (m \text{ 是整数}),$$

于是有
$$3-5y=7m.$$

于是
$$y=\frac{1}{5}(3-7m)=-m+\frac{1}{5}(3-2m).$$

因此要使上式 y 的值是整数，只需找出使 $(3-2m) \vdots 5$ 的整数 m. 显然，这可以取 $m=-1$.

根据
$$y=\frac{1}{5}(3-7m), \quad x=\frac{1}{7}(213-19y),$$

得到：
$$y=\frac{1}{5}[3-7(-1)]=2,$$

$$x=\frac{1}{7}(213-19\cdot 2)=25.$$

因此方程的一切整数解可由下面的公式给出：

$$x=25-9t,\quad y=2+7t.\ (t\text{ 是整数})$$

例 3 求方程 $15x+28y=185$ 的整数解.

把原方程变形成：$x=\frac{1}{15}(185-28y)$

$$=(12-2y)+\frac{1}{15}(5+2y).$$

[这样的变形，比"$x=(12-y)+\frac{1}{15}(5-13y)$"在以后的运算上要来得方便.]

由 y 的整数值，要得出对应的整数值 x，那末$\frac{1}{15}(5+2y)$ 必须是整数.

設 $$\frac{1}{15}(5+2y)=m.\ (m\text{ 是整数})$$

于是得：$$y=\frac{1}{2}(15m-5)$$

$$=(7m-2)+\frac{1}{2}(m-1).$$

很明显，当 $m=1$ 时，$y=5$. 于是

$$x=(12-2\cdot5)+\frac{1}{15}(5+2\cdot5)=3.$$

因此方程的一切整数解，可以由下面的公式给出：

$$x=3-28t,\quad y=5+15t.\ (t\text{ 是整数})$$

例 4 求方程 $23x+53y=109$ 的整数解.

把原方程变形成：$x=\frac{1}{23}(109-53y)$

$$=(5-2y)-\frac{1}{23}(6+7y).$$

当 y 的值是整数时，要使 x 的值也是整数，必須

$$6+7y \vdots 23.$$

今設 $$\frac{1}{23}(6+7y)=m.\ (m\text{是整数})$$

于是得: $$y=\frac{1}{7}(23m-6)$$

$$=(3m-1)+\frac{1}{7}(2m+1).$$

要使 $2m+1 \vdots 7$，可以取 $m=3$. 这样,

$$y=(9-1)+\frac{1}{7}(2\cdot3+1)=9,$$

$$x=5-18-3=-16.$$

因此方程的一切整数解可由下面的公式給出:

$$x=-16-53t,\quad y=9+23t.\ (t\ \text{是整数})$$

例 5 求方程 $7x+9y=35$ 的整数解.

方程两边各除以 7，得

$$x+\frac{9}{7}y=5.$$

要得出一組 x、y 的整数值，必須 $9y \vdots 7$. 这显然只要取 $y=0$ 就合适了. 于是 $x=5$.

因此方程的一切整数解可由下面的公式給出:

$$x=5-9t,\quad y=7t.\ (t\ \text{是整数})$$

讀了下一章的关于連分数的应用后，可以知道整系数二元一次方程一組特殊整数解的一般求法.

4. 方程 $ax+by=c$ 的非負整数解的組数問題

設整系数方程

$$ax+by=c\ (\text{不妨設}\ a>0) \qquad \text{(I)}$$

的一組特殊的整数解是 x_0、y_0，于是

$$x=x_0-bt,\quad y=y_0+at.\ (t\ \text{是整数})$$

为了使 x、y 得到非負值，应使下面两不等式成立:

$$x_0-bt\geqslant 0,\quad y_0+at\geqslant 0.$$

也就是 $$bt\leqslant x_0,\qquad at\geqslant -y_0. \tag{II}$$

下面进行这方面的討論．

(1) 当 $b<0$ 的时候：

因为 $b<0$，于是由(II)得到：$t\geqslant\frac{x_0}{b}$，$t\geqslant -\frac{y_0}{a}$．很明显，适合上面两个同向不等式的整数值 t 可找出无限个，这就得到了方程(I)的无限組非負整数解．因此当 $b<0$ 的时候，方程(I)的非負整数解有无限多組．

(2) 当 $b>0$ 的时候：

(i) 如果 $c<0$，显然，方程(I)沒有非負整数解．

(ii) 如果 $c=0$，那末方程(I)有且仅有一組非負整数解：$x=0$，$y=0$．

(iii) 如果 $c>0$；

我們注意： $$ax_0+by_0=c>0.$$

那末 $$ax_0>-by_0.$$

因为 a、b 都大于 0，所以得：

$$\frac{x_0}{b}>-\frac{y_0}{a}.$$

另一方面，因为 a、b 都大于 0，由(II)可得：

$$t\leqslant\frac{x_0}{b},\quad t\geqslant-\frac{y_0}{a}.$$

于是 $$\frac{x_0}{b}\geqslant t\geqslant-\frac{y_0}{a}. \tag{III}$$

这就表示，当 t 的值取 $-\frac{y_0}{a}$ 与 $\frac{x_0}{b}$ 之間的某一整数的时候，方程(I)就可得到一組非負整数解．因此这时方程(I)的非負整数解的組数，就是 $-\frac{y_0}{a}$ 与 $\frac{x_0}{b}$ 之間的整数的个数（当然，如果 $-\frac{y_0}{a}$ 与 $\frac{x_0}{b}$ 之間不存在

整数，这就表示方程(I)沒有非負整数解).

例如，可断言方程 $2x-3y=17$ 有无限組非負整数解。

因为这里 $b=-3<0$，而 $a=2>0$.

又如，可断言方程 $4x+5y=-7$ 沒有非負整数解.

因为这里 $a=4>0$，$b=5>0$，而 $c=-7<0$.

再如，方程 $4x+5y=0$ 有且仅有一組非負整数解:

$$x=0, \quad y=0.$$

例 1 求方程 $3x+7y=55$ 的非負整数解的組数.

我們能够找到它的一組特殊的整数解是:

$$x_0=16, \quad y_0=1.$$

代入(III)，即得:

$$-\frac{1}{3}\leqslant t\leqslant 2\frac{2}{7}.$$

显然，适合上式的整数值 t 有且仅有下面的三个:

$$0、\ 1、\ 2.$$

因此方程有 3 組非負整数解.

如果以 0、1、2 分别替代以下公式中的 t，

$$x=x_0-bt, \quad y=y_0+at.$$

于是得三組非負整数解如下:

$$\begin{cases}x=16,\\ y=1;\end{cases}\qquad \begin{cases}x=9,\\ y=4;\end{cases}\qquad \begin{cases}x=2,\\ y=7.\end{cases}$$

例 2 求方程 $5x+4y=3$ 的非負整数解.

容易找出它的一組整数解: $x_0=-1$，$y_0=2$.代入(III)，即得:

$$-\frac{2}{5}\leqslant t\leqslant -\frac{1}{4}.$$

显然，沒有整数值 t 能适合上式，因此原方程沒有非負整数解.

对于整系数二元一次方程的非負整数解的組数問題，有下面的定理可以利用.

在叙述定理之前，我們先熟悉一下几个有关的概念．

記号 $[A]$ 表示：不大于实数 A 的最大整数．例如，$\left[4\frac{1}{6}\right]=4$，$[5]=5$，$\left[\frac{2}{3}\right]=0$，$\left[-\frac{5}{2}\right]=-3$，$[\sqrt{2}]=1$，$[-\pi]=-4$ 等等．

显然，整数 $[A]$ 与实数 A 之間具有下列关系：

$$[A]\leqslant A<[A]+1.$$

如果設 $A=[A]+a$（显然，$0\leqslant a<1$），非負数 a 也叫做实数 A 的小数部分，記作 $\{A\}$．

例如： $\left\{4\frac{1}{6}\right\}=\frac{1}{6}$，$\{\sqrt{2}\}=\sqrt{2}-1$ 等等．

这里不准备展开有关这个概念的討論，而仅提出下面的性質：如果 a、b、……、l 都是实数，那末

$$[a+b+\cdots\cdots+l]\geqslant[a]+[b]+\cdots\cdots+[l].$$

証明 因为

$$a=[a]+\{a\},\quad b=[b]+\{b\},\cdots\cdots,\quad l=[l]+\{l\},$$

那末 $[a+b+\cdots\cdots+l]$

$$=[([a]+[b]+\cdots\cdots+[l])+(\{a\}+\{b\}+\cdots\cdots+\{l\})]$$

$$=[a]+[b]+\cdots\cdots+[l]+[\{a\}+\{b\}+\cdots\cdots+\{l\}].$$

因为 $[\{a\}+\{b\}+\cdots\cdots+\{l\}]\geqslant 0$，所以得：

$$[a+b+\cdots\cdots+l]\geqslant[a]+[b]+\cdots\cdots+[l].$$

定理 方程 $$ax+by=c \tag{I}$$

$[a、b、c$ 是正整数，且 $(a,b)=1]$

的非負整数解的組数是：

$$\left[\frac{c}{ab}\right] \text{ 或 } \left[\frac{c}{ab}\right]+1.$$

証明 設 x_0、y_0 是方程(I)的一組特殊整数解．已經知道，要求方程(I)的非負整数解，只需取整数値 t，使下面的不等式成立：

$$-\frac{y_0}{a} \leqslant t \leqslant \frac{x_0}{b}. \tag{II}$$

显然，方程(Ⅰ)非負整数解的組数，就是适合上式的整数值 t 的个数．下面进行討論．

(1) 如果 $-\frac{y_0}{a}$ 是整数：

这时适合(Ⅱ)的整数值 t 的个数是：

$$\left[\frac{x_0}{b}-\left(-\frac{y_0}{a}\right)\right]+1$$

$$=\left[\frac{ax_0+by_0}{ab}\right]+1$$

$$=\left[\frac{c}{ab}\right]+1.$$

因此当 $-\frac{y_0}{a}$ 是整数时，方程(Ⅰ)的非負整数解的組数是：

$$\left[\frac{c}{ab}\right]+1.$$

(2) 如果 $-\frac{y_0}{a}$ 不是整数：

設 $$-\frac{y_0}{a}=\left[-\frac{y_0}{a}\right]+\alpha. \quad (0<\alpha<1)$$

这时，要求适合(Ⅱ)的 t 的整数值个数，便只需求适合下式的 t 的整数值个数：

$$\left[-\frac{y_0}{a}\right]+1 \leqslant t \leqslant \frac{x_0}{b}.$$

因此 t 可取的整数值个数是：

$$\left[\frac{x_0}{b}-\left(\left[-\frac{y_0}{a}\right]+1\right)\right]+1$$

$$=\left[\frac{x_0}{b}-\left(-\frac{y_0}{a}-\alpha+1\right)\right]+1$$

$$=\left[\frac{ax_0+by_0}{ab}+\alpha-1\right]+1$$

$$=\left[\frac{c}{ab}+\alpha\right]-1+1=\left[\frac{c}{ab}+\alpha\right].$$

設 $\frac{c}{ab}=\left[\frac{c}{ab}\right]+p$ $(0\leqslant p<1)$，因此

$$\left[\frac{c}{ab}+\alpha\right]=\left[\left[\frac{c}{ab}\right]+p+\alpha\right]$$

$$=\left[\frac{c}{ab}\right]+[\alpha+p].$$

因为 $0<\alpha<1$，$0\leqslant p<1$，于是 $0<\alpha+p<2$. 因此如果 $\alpha+p\geqslant 1$，t 可取的整数值 t 的个数是：$\left[\frac{c}{ab}\right]+1$.

也就是說，方程(I)的非負整数解的組数是：$\left[\frac{c}{ab}\right]+1$.

如果 $\alpha+p<1$，t 可取的整数值 t 的个数是：$\left[\frac{c}{ab}\right]$.

也就是說，方程(I)的非負整数解的組数是：$\left[\frac{c}{ab}\right]$.

例 1 决定方程 $3x+7y=55$ 的非負整数解的組数.

已知 $x_0=16$，$y_0=1$ 是方程的一組特殊整数解.这里

$$-\frac{y_0}{a}=-\frac{1}{3}=-1+\frac{2}{3}，\text{即 } \alpha=\frac{2}{3}.$$

而
$$\frac{c}{ab}=\frac{55}{21}=2+\frac{13}{21}，\text{即 } p=\frac{13}{21}.$$

由于 $\alpha+p=\frac{2}{3}+\frac{13}{21}=\frac{27}{21}>1$，因此方程的非負整数解的組数是：

$$\left[\frac{c}{ab}\right]+1=2+1=3.$$

例 2 决定方程 $5x+4y=3$ 的非負整数解的組数.

已知 $x_0=-1$, $y_0=2$ 是方程的一組特殊的整数解.

这里 $-\frac{y_0}{a}=-\frac{2}{5}=-1+\frac{3}{5}$, 即 $\alpha=\frac{3}{5}$.

而 $\frac{c}{ab}=\frac{3}{20}=0+\frac{3}{20}$, 即 $p=\frac{3}{20}$.

由于 $\alpha+p=\frac{3}{5}+\frac{3}{20}<1$, 因此方程的非負整数解的組数是:

$$\left[\frac{c}{ab}\right]=0.$$

多元的整系数一次方程的整数解問題，可以归結成两元的整系数一次方程而获得解决．这里对它不再作深入的探討，仅提供下面的定理:

整系数方程

$$a_1x_1+a_2x_2+\cdots\cdots+a_nx_n=c_n \qquad (\text{I})$$

存在整数解的充分而且必要条件是:

$$c_n \vdots d_n. \quad [d_n=(|a_1|, |a_2|, \cdots\cdots, |a_n|)]$$

証明 关于条件的必要性的証明极簡单.

如果方程（I）具有整数解 u_1、u_2、……、u_n, 又設 $a_1=d_nq_1$, $a_2=d_nq_2$, ……, $a_n=d_nq_n$.（这里 q_i 是非零整数）于是,

$$d_n(q_1u_1+q_2u_2+\cdots\cdots+q_nu_n)=c_n.$$

这样 $c_n \vdots d_n$.

关于条件的充分性:应用数学归納法.

(1) 当 $n=2$ 的时候,断言显然成立.

(2) 当 $n=k$ 的时候,如果断言成立,即假定: 当 $c_k \vdots d_k$ 的时候,方程 $a_1x_1+a_2x_2+\cdots\cdots+a_kx_k=c_k$ 有整数解.

我們証明: 当 $n=k+1$ 的时候, 断言也成立. 也就是証明: 当 $c_{k+1} \vdots d_{k+1}$ 的时候,方程

$$a_1x_1+a_2x_2+\cdots\cdots+a_kx_k+a_{k+1}x_{k+1}=c_{k+1} \qquad (\text{II})$$

也有整数解.

因为 $d_k=(|a_1|, |a_2|, \cdots\cdots, |a_k|)$，所以

$$d_{k+1}=(|a_1|, \cdots\cdots, |a_k|, |a_{k+1}|)=(d_k, |a_{k+1}|).$$

而 $c_{k+1} \vdots d_{k+1}$，因此下面的方程有整数解：

$$d_k x+a_{k+1}x_{k+1}=c_{k+1}. \qquad \text{(III)}$$

設这个方程的一組整数解是：t、u。

另一方面，由假設知道

$$a_1x_1+a_2x_2+\cdots\cdots+a_kx_k=c_k$$

有整数解．設这組解是：v_1、v_2、……、v_k．也就是

$$d_k=a_1v_1+a_2v_2+\cdots\cdots+a_kv_k.$$

把上面的結果代入(III)得：

$$a_1(v_1t)+a_2(v_2t)+\cdots\cdots+a_k(v_kt)+a_{k+1}u=c_{k+1}.$$

設 $u_1=v_1t$, $u_2=v_2t$, ……, $u_k=v_kt$, $u_{k+1}=u$，显然，u_1、u_2、……、u_k、u_{k+1} 也就是方程(II)的整数解．

綜合上述，也就是証明了定理的成立．

§2　三边是整数的直角三角形的解

方程 $x^2+y^2=z^2$ 的正整数解的几何意义就是三边都是整数值的直角三角形．

对于 $x^2+y^2=z^2$ 如果 $(x, y)=d>1$，那末 d 也一定是 z 的約数．

因此求方程 $x^2+y^2=z^2$ 的正整数解，可設 $(x, y)=1$ [这样，可推知 $(y, z)=1$, $(z, x)=1$]．

容易指出 x、y 中必有一偶数．不然，如果 x 和 y 都是奇数，那末 $x^2\equiv y^2\equiv 1 \pmod 4$．也就是 $x^2+y^2\equiv 2 \pmod 4$．然而不論 z 的值是奇数还是偶数，总不可能有 $z^2\equiv 2 \pmod 4$．这就指出了 x、y 中一定有一个是偶数．显然，其余的两个应該都是奇数．

定理　方程　　$x^2+y^2=z^2$　　(I)

[这里 $(x, y)=1$，且設 x 是偶数]

的正整数解，一定可以表示成：

$$x=2mn,\quad y=m^2-n^2,\quad z=m^2+n^2. \tag{II}$$

[这里 m、n 是正整数，$m>n$，$(m, n)=1$，且 m、n 中一个是奇数，一个是偶数.]

反过来，形如(II)的三个数，一定适合方程(I).

證明

(I)可以变形成：　$x^2=(z+y)(z-y)$.

因为 $z+y$，$z-y$ 是偶数，所以

$$\left(\frac{x}{2}\right)^2=\frac{z+y}{2}\cdot\frac{z-y}{2}, \tag{III}$$

而 $\frac{z+y}{2}$，$\frac{z-y}{2}$ 都是正整数，且

$$\left(\frac{z+y}{2},\ \frac{z-y}{2}\right)=(z,\ y)=1.$$

因此，当也只当下面的条件下，(III)才成立.就是，

$$\frac{z+y}{2}=m^2,\quad \frac{z-y}{2}=n^2.$$

[这里 m、n 是正整数，$m>n$，且 $(m, n)=1$]

因为 $m^2+n^2=z$，而 z 是奇数，因此在 m、n 中必須有一个是奇数，另一个是偶数.

綜合上述，就得(II)；

$$x=2mn,\quad y=m^2-n^2,\quad z=m^2+n^2.$$

[这里 m、n 是正整数，$m>n$，$(m, n)=1$，且 m、n 中有一个是奇数，一个是偶数.]

反过来，形如(II)的三个数，一定适合(I)：

因为　$x^2+y^2=(2mn)^2+(m^2-n^2)^2$

$$=m^2+n^2=z^2.$$

应該指出，数組 m、n 与数組 x、y、z 是一一对应的：

不同的数組 m、n 对应着不同的数組 x、y、z. 关于这一点是极明显的.反过来，如果数組 x、y、z 对应着数組 m、n，又对应着数組 m_1、

n_1，于是

$$x=2mn,\quad y=m^2-n^2,\quad z=m^2+n^2;$$

同时，
$$x=2m_1n_1,\ y=m_1^2-n_1^2,\ z=m_1^2+n_1^2.$$

由
$$\frac{y+z}{2}=m^2,\quad \frac{y+z}{2}=m_1^2,$$

得到
$$m^2=m_1^2.$$

既然 m、m_1 都是正整数，因此 $m=m_1$. 同理可証 $n=n_1$.

譬如：

以 $m=2$, $n=1$ 代入(II)，得到方程(I)的一組正整数解是：

$$x=4,\quad y=3,\quad z=5.$$

以 $m=3$, $n=2$ 代入(II)，得到方程(I)的一組正整数解是：

$$x=12,\quad y=5,\quad z=13.$$

以 $m=4$, $n=3$ 代入(II)，得到方程(I)的一組正整数解是：

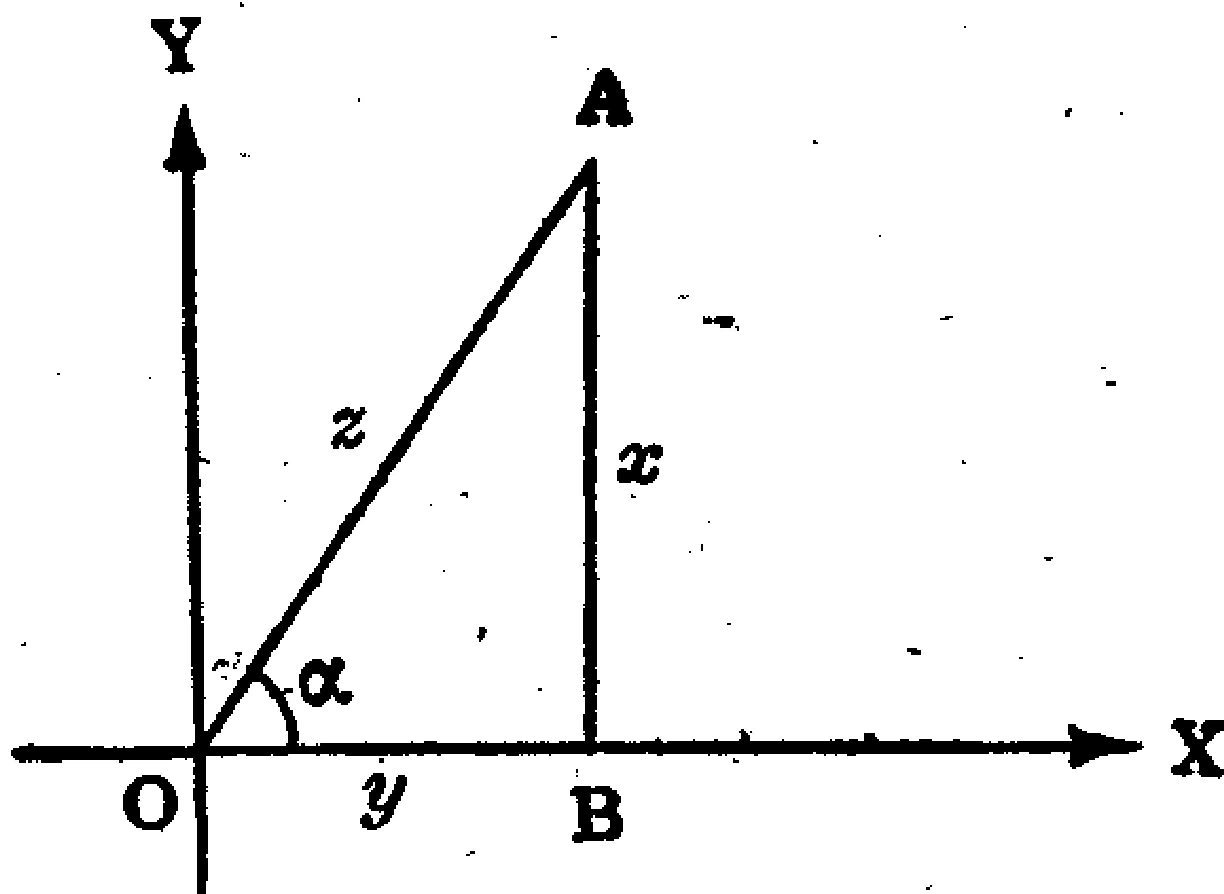
$$x=24,\quad y=7,\quad z=25.$$

下面再介紹一种三边是整数的直角三角形的解的公式.

我們知道，对于实数 t，一定能找到 $\frac{\alpha}{2}$，使

$$\operatorname{tg}\frac{\alpha}{2}=t.$$

作綫段 OA，使与坐标軸 OX 的夹角为 α，由 A 点作 OX 的垂綫，設垂足为 B. 于是构成了直角三角形 AOB.



設 $OA=z$, $AB=x$, $OB=y$，那末

$$x=z\sin\alpha,\quad y=z\cos\alpha.$$

于是，
$$\sin\alpha=\frac{2\operatorname{tg}\frac{\alpha}{2}}{1+\operatorname{tg}^2\frac{\alpha}{2}}=\frac{2t}{1+t^2},$$

$$\cos\alpha=\frac{1-\operatorname{tg}^2\frac{\alpha}{2}}{1+\operatorname{tg}^2\frac{\alpha}{2}}=\frac{1-t^2}{1+t^2},$$

因此，
$$x=\frac{2t}{1+t^2}\cdot z;\quad y=\frac{1-t^2}{1+t^2}\cdot z.$$

这样就得到如下的公式：

$$\frac{x}{2t}=\frac{y}{1-t^2}=\frac{z}{1+t^2}.$$

如果取 t 是整数($t\neq 0$、1、-1)，由上式就可以得到三边为整数的直角三角形的解.

注 我們是以 $|x|$、$|y|$、$|z|$ 作为直角三角形三边的.

譬如：取 $t=2$ 的时候，可得到如下的解：

$$x=4,\quad |y|=3,\quad z=5.$$

取 $t=4$ 的时候，可得到如下的解：

$$x=8,\quad |y|=15,\quad z=17.$$

取 $t=5$ 的时候，可得到如下的解：

$$x=5,\quad |y|=12,\quad z=13.$$

取 $t=6$ 的时候，可得到如下的解：

$$x=12,\quad |y|=35,\quad z=37.$$

§3 方程 $x^4+y^4=z^4$ 的正整数解

前面已提到过的17世紀法国大数学家費尔馬（Fermat 1601—1665)曾有过如下的論断(通常叫做費尔馬大定理)：

"方程 $x^n+y^n=z^n$ $(n>2)$没有正整数解."

尽管他自己說有一个証明方法(沒有公开),然而,以后的数学家們对于該論断的証明始終沒有找到.有沒有"証明",到今天还是悬案.[值得指出的是:历代优秀数学家們为了証明这个論断,不知耗費了多少精力.虽然到今天沒有获得徹底解决,可是却得到了另外的收获,就是在数論上开辟了新的园地.例如,数学家庫米尔(Kummer 1810—1893)在証明該論断的过程中,建立了"理想数論".这个发現在数学的发展上起了巨大的作用.]

对于費尔馬定理,极有威望的数学家曾指出:如果想用完全初等的方法来解决,是注定不会成功的.

即使討論的是当 n 是一些特殊数值时,关于定理的証明,也会遇到很大的困难.我們只要看:譬如,欧拉只証明了当 $n=3$、4 时的特殊情形;又如,1823 年勒讓得尔証明了当 $n=5$ 时的特殊情形;1849 年庫米尔証明了当 $n<100$ 时的情形;今天,当 $n<619$(以及后面一系列較大的数值)时,定理也获得了証明.

对于費尔馬大定理,实际上只需討論 $n=4$ 与一切奇質数的情形就够了.如果对于大于 4 的合数 $N=nq$ (n 是質数),方程 $x^N+y^N=z^N$ (即 $x^{nq}+y^{nq}=z^{nq}$) 有正整数解,那末必导致方程 $X^n+Y^n=Z^n$ (这里 $X=x^q$, $Y=y^q$, $Z=z^q$)也有正整数解.这些叙述,就表明了:如果費尔馬大定理对于 n 是某一質数时成立,那末对于一切能被該質数整除的 n,这一定理也一定成立.既然已經知道,当 $n<619$(当然 $n>2$)时,費尔馬大定理是成立的,于是,可推知:費尔馬大定理,对于能被小于 619 的質数整除(或能被 4 整除)的 n 也成立.

下面叙述的是,当 $n=4$ 时,費尔馬大定理的証明、証明的方法是"无穷递降法".这样,剩下的只需研究 n 是奇質数的情形了.

定理 方程 $x^4+y^4=z^4$ 沒有正整数解.

証明 我們只需証明 $x^4+y^4=z^2$ 沒有正整数解.

如果方程
$$x^4+y^4=z^2 \tag{I}$$

具有正整数解. 我們可以只研究 $(x, y)=1$ 的情形, 因为如果 $(x, y)=d>1$, d 必是 z^2 的約数,从而也一定是 z 的約数.

設 x_0、y_0、z_0 是(I)的一組正整数解, $(x_0, y_0)=1$, 于是

$$x_0^4+y_0^4=z_0^2.$$

也就是

$$(x_0^2)^2+(y_0^2)^2=z_0^2.$$

从上节,可知: x_0^2、y_0^2、z_0 可表成如下形式(設 x_0 是偶数):

$$x_0^2=2uv,\quad y_0^2=u^2-v^2,\quad z_0=u^2+v^2.$$

[这里 $u>v>0$, $(u, v)=1$, 且 u、v 中一个是奇数, 一个是偶数] 我們可断言: 这里 u 必是奇数 (当然 v 就一定为偶数了). 这可从 $y_0^2=u^2-v^2$ 得知:

如果 u 是偶数, 也就是 $u^2\equiv 0 \pmod 4$. 因为 v 是奇数, 所以 $v^2\equiv 1 \pmod 4$. 从而 $u^2-v^2\equiv -1 \pmod 4$.

然而, y_0 当然是奇数, 应有 $y_0^2\equiv 1 \pmod 4$. 这与 "$y_0^2=u^2-v^2$" 矛盾.

既然 u 应是奇数, 于是 $(u, 2)=1$. 已知 $(u, v)=1$, 因此得 $(u, 2v)=1$.

由 $x_0^2=u(2v)$, 知 u、$2v$ 非各为完全平方数不可.

設 $u=m^2$, $2v=n^2$, (显然, n 是偶数)再观察 $v^2+y_0^2=u^2$.

这里 v 是偶数,且由 $(v、u)=1$ 可知, $(v, y_0)=1$. 于是再由上节知識,可知 v、y_0、u 有如下形式:

$$v=2ab,\quad y_0=a^2-b^2,\quad u=a^2+b^2.$$

[这里 $a>b>0$, $(a, b)=1$, a、b 中一个是奇数,一个是偶数.]

由 $v=2ab$, 而 $2v=n^2$, 推得

$$\left(\frac{n}{2}\right)^2=ab.$$

因为 n 是偶数,所以上式左边是一完全平方数. 而$(a, b)=1$, 因此非 a、b 分别是平方数不可.

設 $a=p^2$, $b=q^2$. 又知 $u=m^2$, 于是从 $u=a^2+b^2$ 得 $p^4+q^4=m^2$,

也就表示 p、q、m 为(I)的一組正整数解.

而 $$z_0=u^2+v^2>u^2>u=m^2>m.$$

我們用 x_1、y_1、z_1 分别代替 p、q、m 三个数，于是說：如果 x_0、y_0、z_0 是(I)的正整数解，那末一定能找到 x_1、y_1、z_1 也是(I)的正整数解，且 $z_0>z_1$.

可是，有了正整数解 x_1、y_1、z_1，当然又能找到数組 x_2、y_2、z_2 也是(I)的正整数解.且有 $z_0>z_1>z_2$.

按此下去，显然可以找到数組 x_3、y_3、z_3；x_4、y_4、z_4；……；x_n、y_n、z_n；……都是方程(I)的正整数解.且 $z_0>z_1>z_2>\cdots\cdots>z_n>\cdots\cdots$.

事实上，正整数中最小的是 1，所以各項都是正整数的无限递降数列是不存在的.

这个矛盾是由于假定了方程(I)有正整数解而引得的.因此方程(I)沒有正整数解，也就是方程 $x^4+y^4=z^4$ 沒有正整数解.

第八章 連分数

在数的理論中，連分数的应用比較广泛.而且，关于連分数的理論早就有了新的发展.因限于这本書的性质，这里主要介紹了連分数的一些簡单性质以及它在解不定方程上的应用.

§1 連分数的定义

設 α 为任意一实数，以 q_1 表示不超过 α 的最大整数(即 $q_1=[\alpha]$).于是，如果 α 不是整数，可得：

$$\alpha=q_1+\frac{1}{\alpha_2}.\quad (\alpha_2>1)$$

例如：$\dfrac{5}{3}=1+\dfrac{2}{3}$，就是 $\dfrac{5}{3}=1+\dfrac{1}{\dfrac{3}{2}}$；

$$-\frac{5}{3}=-2+\frac{1}{3};$$

$$\sqrt{2}=1+(\sqrt{2}-1)=1+\frac{1}{\sqrt{2}+1}.$$

如果 a_2 不是整数，同样又可得：

$$a_2=q_2+\frac{1}{a_3}. \quad (a_3>1)$$

依次类推，就可得到下列一系列等式：

$$a_3=q_3+\frac{1}{a_4}, \quad (a_4>1)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$a_{n-1}=q_{n-1}+\frac{1}{a_n}. \quad (a_n>1)$$

由上面的一系列等式，得到：

$$\alpha=q_1+\frac{1}{a_2}=q_1+\cfrac{1}{q_2+\cfrac{1}{a_3}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4}}}$$

$$=\cdots\cdots\cdots\cdots\cdots\cdots$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{a_n}}}}.$$

上式叫做简单連分数(以后就叫做連分数)．如果經过有限个步骤能找到自然数 n，而 a_n是整数，那末这种連分数叫做有限連分数．不然，就叫做无限連分数．

这里，整数 q_1、q_2、……，叫做連分数的第一、第二、……个部分分母。

注1 观察連分数的定义，可以知道：q_1 是任意整数，而 q_i（$i=2$、3、……）是正整数。

注2 为了使任一有限連分数有它确定的形式，对于有限連分数，可以规定它的最后的分母大于1．不然，对于有限連分数

$$q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}$$

还可写成如下的形式：

$$q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{(q_{n-1}-1)+\cfrac{1}{1}}}}.$$

根据定义，任一实数必能以連分数来表示．事实上，任一实数也只能以唯一的一个連分数来表示．这个断言，証明如下：

如果实数
$$\alpha=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}},$$

又
$$\alpha=p_1+\cfrac{1}{p_2+\cfrac{1}{p_3+\ddots}}.$$

我們証明：$q_i=p_i$（$i=1$、2、3、……）．

証明 应用数学归納法．

（1）显然，$q_1=p_1$．如果 $q_1\neq p_1$，在整数 q_1、p_1 上各加上一个非負但小于1的数，結果当然还是不等．于是就导致 $\alpha\neq\alpha$．

(2) 假設 $q_k=p_k$ ($k=1、2、\cdots\cdots、n-1$)，我們証明:

$$q_n=p_n.$$

由假設 $q_k=p_k$ 可知:

$$q_1+\cfrac{1}{q_2+\cfrac{}{\ddots+\cfrac{1}{q_{n-1}}}}=p_1+\cfrac{1}{p_2+\cfrac{}{\ddots+\cfrac{1}{p_{n-1}}}}.$$

如果 $q_n\neq p_n$，显然,

$$q_n+\cfrac{1}{q_{n+1}+\ddots}\neq p_n+\cfrac{1}{p_{n+1}+\ddots}.$$

这样,就导致

$$q_1+\cfrac{1}{q_2+\cfrac{}{\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n+\cfrac{1}{q_{n+1}+\ddots}}}}}$$

$$\neq p_1+\cfrac{1}{p_2+\cfrac{}{\ddots+\cfrac{1}{p_{n-1}+\cfrac{1}{p_n+\cfrac{1}{p_{n+1}+\ddots}}}}}.$$

即 $\alpha\neq\alpha$.

綜合上述,也就証明了 $q_i=p_i$ ($i=1、2、3、\cdots\cdots$).

§2 有限連分数与欧几里德除法的联系

定理 有理数一定能用有限連分数来表示.

証明 我們只需注意正有理数的情形,因为如果 α 是負有理数,那

末一定可以写成 $\alpha=[\alpha]+\beta$，而 β 是正有理数.

設 $\frac{a}{b}$ $[(a, b)=1]$ 表示一正有理数. 我們知道，对于 a、b，存在如下的有限个等式:

$$
\left.\begin{array}{ll}
a=bq_1+r_2; & (0<r_2<b)\\
b=r_2q_2+r_3; & (0<r_3<r_2)\\
r_2=r_3q_3+r_4; & (0<r_4<r_3)\\
\cdots\cdots\cdots\cdots\cdots; & \cdots\cdots\cdots\cdots\cdots\\
r_{n-2}=r_{n-1}q_{n-1}+r_n; & (0<r_n<r_{n-1})\\
r_{n-1}=r_nq_n.
\end{array}\right\} \quad \text{(I)}
$$

把(I)中每一等式分别改写成如下的形式:

$$
\left.\begin{array}{l}
\dfrac{a}{b}=q_1+\dfrac{1}{\dfrac{b}{r_2}};\\[2ex]
\dfrac{b}{r_2}=q_2+\dfrac{1}{\dfrac{r_2}{r_3}};\\[2ex]
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots;\\[1ex]
\dfrac{r_{n-2}}{r_{n-1}}=q_{n-1}+\dfrac{1}{\dfrac{r_{n-1}}{r_n}};\\[2ex]
\dfrac{r_{n-1}}{r_n}=q_n.
\end{array}\right\}
$$

观察上面的等式組，可以看到相邻两个等式之間的关系，于是得到:

$$
\frac{a}{b}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}}.
$$

这就証明了有理数$\frac{a}{b}$能用有限連分数表示.

由定理可以得到把有理数化成連分数的方法：因为对于正整数 a、b，如下的形式就包含着(I)中的 n 个等式.

	a	b	q_1
	bq_1	r_2q_2	
q_2	r_2	r_3	q_3
	r_3q_3	r_4q_4	
q_4	r_4	r_5	q_5
……	………	………	……
q_{n-2}	r_{n-2}	r_{n-1}	q_{n-1}
	$r_{n-1}q_{n-1}$	r_nq_n	
q_n	r_n	0	

例 1 把$\frac{50}{13}$化成連分数.

	50	13	3
	39	11	
1	11	2	5
	10	2	
2	1	0	

由左边，可知：

$$\frac{50}{13}=3+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{2}}}.$$

例 2 把$\frac{17}{40}$化成連分数.

	17	40	0
	0	34	
2	17	6	2
	12	5	
1	5	1	5
	5		
	0		

由左边，可知：

$$\frac{17}{40}=\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{5}}}}.$$

例3 把 $-\frac{15}{13}$ 化成連分数.

因为 $-\frac{15}{13}=-2+\frac{11}{13}$，而

$$\frac{11}{13}=\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{2}}},$$

所以

$$-\frac{15}{13}=-2+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{2}}}.$$

順便，可以知道：有限連分数的值一定是确定的有理数．这是因为有限連分数可以化成一个普通分数．

§3 近似分数的性质

近似分数的定义：

$$\delta_1=q_1;$$

$$\delta_2=q_1+\frac{1}{q_2};$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\delta_n=q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n}}}.$$

是連分数

$$q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n+\ddots}}} \qquad \text{(I)}$$

的第一、第二、……、第 n 个近似分数.

注 1 如果把 δ_n 中的 q_n 以 $q_n+\dfrac{1}{q_{n+1}}$ 来代替,就得到了 δ_{n+1}.

注 2 有限連分数的末一个近似分数,就等于連分数的値.这时我們把不是末一个的近似分数叫做連分数的眞近似分数.

例如,連分数

$$3+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2}}}.$$

$$\delta_1=3;\quad \delta_2=3+\frac{1}{2}=\frac{7}{2};$$

$$\delta_3=3+\cfrac{1}{2+\cfrac{1}{1}}=3+\frac{1}{3}=\frac{10}{3};$$

$$\delta_4=3+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2}}}=3+\cfrac{1}{2+\cfrac{2}{3}}=\frac{27}{8}.$$

(这里 δ_4 就是連分数的値)

又如,連分数

$$\cfrac{1}{5+\cfrac{1}{3+\cfrac{1}{2}}}$$

的近似分数 $\delta_1=0$.

对于連分数的近似分数的概念,介紹如下的几条定理.

定理 1 連分数

$$q_1+\cfrac{1}{q_2+\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n+\ddots}}}$$

的近似分数的分子分母构成規則如下：

設 $\delta_1=\frac{P_1}{Q_1}$，$\delta_2=\frac{P_2}{Q_2}$，……，$\delta_k=\frac{P_k}{Q_k}$，

那末
$$P_k=P_{k-1}q_k+P_{k-2},\quad Q_k=Q_{k-1}q_k+Q_{k-2}.\qquad (k\geqslant 3)$$

証明 应用数学归納法.

首先，
$$\delta_1=\frac{q_1}{1}，就是 P_1=q_1,\ Q_1=1.$$

$$\delta_2=q_1+\frac{1}{q_2}=\frac{q_1q_2+1}{q_2},$$

于是
$$P_2=q_1q_2+1,\quad Q_2=q_2.$$

$$\delta_3=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}=\frac{q_1q_2q_3+q_1+q_3}{q_2q_3+1},$$

于是
$$P_3=q_1q_2q_3+q_1+q_3,\quad Q_3=q_2q_3+1.$$

很明显，
$$P_3=(q_1q_2+1)q_3+q_1=P_2q_3+P_1,$$

而
$$Q_3=Q_2q_3+Q_1.$$

上面驗証了当 $k=3$ 的时候，定理是成立的.

其次，假設当 $k=t$ 的时候，定理也成立，就是

$$P_t=P_{t-1}q_t+P_{t-2},$$

而
$$Q_t=Q_{t-1}q_t+Q_{t-2}.$$

我們証明，当 $t=k+1$ 的时候，定理仍然成立，就是証明：

$$P_{t+1}=P_tq_{t+1}+P_{t-1},$$

$$Q_{t+1}=Q_tq_{t+1}+Q_{t-1}.$$

因为
$$\delta_t=\frac{P_t}{Q_t}=\frac{P_{t-1}q_t+P_{t-2}}{Q_{t-1}q_t+Q_{t-2}},$$

我們知道，如果将 δ_t 中的 q_t 用 $q_t+\frac{1}{q_{t+1}}$ 来代替，就得 δ_{t+1}. 所以

$$\delta_{t+1}=\frac{P_{t-1}\left(q_t+\dfrac{1}{q_{t+1}}\right)+P_{t-2}}{Q_{t-1}\left(q_t+\dfrac{1}{q_{t+1}}\right)+Q_{t-2}}$$

$$=\frac{P_{t-1}q_t+P_{t-2}+\dfrac{P_{t-1}}{q_{t+1}}}{Q_{t-1}q_t+Q_{t-2}+\dfrac{Q_{t-1}}{q_{t+1}}}$$

$$=\frac{P_t+\dfrac{P_{t-1}}{q_{t+1}}}{Q_t+\dfrac{Q_{t-1}}{q_{t+1}}}=\frac{P_tq_{t+1}+P_{t-1}}{Q_tq_{t+1}+Q_{t-1}}.$$

也就是說，

$$P_{t+1}=P_tq_{t+1}+P_{t-1},$$

$$Q_{t+1}=Q_tq_{t+1}+Q_{t-1}.$$

于是，定理得証.

例 連分数

$$3+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{5}}}}.$$

因为 $\delta_1=\frac{3}{1}$，$\delta_2=3+\frac{1}{2}=\frac{7}{2}$，于是得到

$$P_1=3,\quad Q_1=1;\qquad P_2=7,\quad Q_2=2.$$

所以

$$P_3=P_2q_3+P_1=7\cdot3+3=24,$$

$$Q_3=Q_2q_3+Q_1=2\cdot3+1=7;$$

$$P_4=P_3q_4+P_2=24\cdot4+7=103,$$

$$Q_4=Q_3q_4+Q_2=7\cdot4+2=30;$$

$$P_5=P_4q_5+P_3=103\cdot5+24=539,$$

$$Q_5=Q_4q_5+Q_3=30\cdot5+7=157;$$

因此，$\delta_3=\frac{24}{7}$，$\delta_4=\frac{103}{30}$，$\delta_5=\frac{539}{157}$.

推論 当 $n\geqslant 3$ 的时候，近似分数 δ_n 的分母

$$Q_n\geqslant n-1.$$

証明 因为 $Q_n=Q_{n-1}q_n+Q_{n-2}$，又 $q_n\geqslant 1$，$Q_{n-2}\geqslant 1$，所以

$$Q_n\geqslant Q_{n-1}+1.$$

这就可用数学归納法来証明：

(1) 当 $n=3$ 的时候，因为 $Q_3=Q_2q_3+1=q_2q_3+1$，又 $q_2\geqslant 1$，$q_3\geqslant 1$，所以 $Q_3\geqslant 2$. 也就是这时断言是成立的.

(2) 設 $Q_k\geqslant k-1$，求証：$Q_{k+1}\geqslant k$.

因为 $Q_{k+1}\geqslant Q_k+1$，而 $Q_k\geqslant k-1$，因此証实了：

$$Q_{k+1}\geqslant k.$$

定理 2 連分数

$$q_1+\cfrac{1}{q_2+\cfrac{}{\ddots+\cfrac{1}{q_{n-1}+\cfrac{1}{q_n+\ddots}}}}$$

的相邻两近似分数 δ_{k-1} 与 δ_k 間有着如下的关系：

$$\delta_k-\delta_{k-1}=\frac{(-1)^k}{Q_kQ_{k-1}}.\quad(k>1)$$

$$[\text{或 } P_kQ_{k-1}-Q_kP_{k-1}=(-1)^k]$$

証明 应用数学归納法証明.

(1) 当 $k=2$ 的时候，定理是成立的. 因为

$$\delta_2=\frac{q_1q_2+1}{q_2},\quad \delta_1=\frac{q_1}{1}.$$

于是 $Q_2=q_2$，$Q_1=1$，因此

$$\delta_2-\delta_1=\frac{q_1q_2+1}{q_2}-\frac{q_1}{1}$$

$$=\frac{1}{q_2\cdot 1}$$

$$=\frac{(-1)^2}{Q_2Q_1}.$$

(2) 設 $k=t$ 的时候，定理成立，就是

$$\delta_t-\delta_{t-1}=\frac{(-1)^t}{Q_tQ_{t-1}}.$$

我們証明，当 $k=t+1$ 的时候，定理仍然成立．就是証明：

$$\delta_{t+1}-\delta_t=\frac{(-1)^{t+1}}{Q_{t+1}Q_t}.$$

因为 $$\delta_{t+1}-\delta_t=\frac{P_{t+1}Q_t-P_tQ_{t+1}}{Q_{t+1}Q_t}$$

$$=\frac{(P_tq_{t+1}+P_{t-1})Q_t-P_t(Q_tq_{t+1}+Q_{t-1})}{Q_{t+1}Q_t}$$

$$=\frac{P_{t-1}Q_t-P_tQ_{t-1}}{Q_{t+1}Q_t}$$

$$=\frac{(-1)\cdot(P_tQ_{t-1}-P_{t-1}Q_t)}{Q_{t+1}Q_t},$$

由 $\delta_t-\delta_{t-1}=\dfrac{(-1)^t}{Q_tQ_{t-1}}$，因此 $P_tQ_{t-1}-P_{t-1}Q_t=(-1)^t$．于是得：

$$\delta_{t+1}-\delta_t=\frac{(-1)\cdot(-1)^t}{Q_{t+1}Q_t}=\frac{(-1)^{t+1}}{Q_{t+1}Q_t}.$$

这就証明了定理的成立．

例如，連分数

$$2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{2}}}},$$

由定理1,可以計算出近似分数:

$$\delta_4=\frac{47}{17},\quad \delta_5=\frac{105}{38}.$$

根据上面的定理，可断言 $\delta_5-\delta_4=\frac{(-1)^5}{17\cdot 38}=-\frac{1}{17\cdot 38}$. 事实上,

$$\delta_5-\delta_4=\frac{105}{38}-\frac{47}{17}=\frac{105\cdot 17-47\cdot 38}{38\cdot 17}=\frac{-1}{38\cdot 17}.$$

推論 $\delta_k=\frac{P_k}{Q_k}$是既約分数.

証明 由定理知:

$$P_kQ_{k-1}-P_{k-1}Q_k=(-1)^k.$$

如果$(P_k,\ Q_k)=d>1$, 那末一定导致$(-1)^k\ \vdots\ d$. 这是不合理的. 因此

$$(P_k,\ Q_k)=1.$$

定理3 設 δ_n 是无限連分数

$$q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}}$$

的第 n 个近似分数, 那末 $\lim\limits_{n\to\infty}\delta_n$ 存在.

証明 首先証明:

$$\delta_{2k+1}<\delta_{2k}; \tag{1}$$

$$\delta_{2k-1}<\delta_{2k+1}; \tag{2}$$

$$\delta_{2k-2}>\delta_{2k}. \tag{3}$$

注 这三个結論,对于有限連分数也同样适用.

由定理2知:

$$\delta_{2k+1}-\delta_{2k}=\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}}<0.$$

这就証实了(1).

因为 $\delta_{2k+1}-\delta_{2k}=\frac{-1}{Q_{2k+1}Q_{2k}}$， 而 $\delta_{2k}-\delta_{2k-1}=\frac{1}{Q_{2k}Q_{2k-1}}$，所以

$$\delta_{2k+1}-\delta_{2k-1}=\frac{Q_{2k+1}-Q_{2k-1}}{Q_{2k+1}Q_{2k}Q_{2k-1}}.$$

又由定理1可推知： $Q_{2k+1}>Q_{2k-1}$.

于是有 $\delta_{2k+1}-\delta_{2k-1}>0$，因此就証实了(2).

同理可以証实(3).

(1)、(2)、(3)表明了：

δ_1、δ_3、δ_5、……、δ_{2n-1} 是递增而有上界的数列.

δ_2、δ_4、δ_6、……、δ_{2n} 是递减而有下界的数列.

所以 $\lim\limits_{n\to\infty}\delta_{2n-1}$ 存在，$\lim\limits_{n\to\infty}\delta_{2n}$ 也存在.

事实上， $$|\delta_{2n}-\delta_{2n-1}|=\frac{1}{Q_{2n}Q_{2n-1}}.$$

由定理1的推論可知：$Q_{2n}\geqslant 2n-1$，$Q_{2n-1}\geqslant 2n-2$，

因此， $$|\delta_{2n}-\delta_{2n-1}|\leqslant\frac{1}{2(n-1)(2n-1)}.$$

显然，对于任意給定的 $\varepsilon>0$，一定能找到正数 N，当 $n>N$ 时，

$$|\delta_{2n}-\delta_{2n-1}|<\varepsilon.$$

这就証明了：

$$\lim_{n\to\infty}\delta_{2n-1}=\lim_{n\to\infty}\delta_{2n}.$$

也就是証明了：$\lim\limits_{n\to\infty}\delta_n$ 是存在的.

既然如此，我們把

$$\alpha=\lim_{n\to\infty}\delta_n$$

当作无限連分数的值，記作

$$\alpha=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots}}.$$

因为极限的存在是唯一的，所以任一无限連分数唯一地对应着一个实数．

这样，綜合§1、§2的知識，可以得到下面的結論：实数与連分数之間存在着一一对应的关系．

定理 4 設連分数的值为α，那末近似分数δ_{k+1}比δ_k更靠近于α，也就是

$$|\alpha-\delta_{k+1}|<|\alpha-\delta_k|.$$

証明 由定理1可得：

$$\delta_{k+1}=\frac{P_{k+1}}{Q_{k+1}}=\frac{P_k q_{k+1}+P_{k-1}}{Q_k q_{k+1}+Q_{k-1}}.$$

容易知道，把δ_{k+1}中的q_{k+1}換之以①

$$q_{k+1}+\cfrac{1}{q_{k+2}+\ddots}$$

就得到連分数的值．

于是

$$\alpha=\frac{P_k\left(q_{k+1}+\cfrac{1}{q_{k+2}+\ddots}\right)+P_{k-1}}{Q_k\left(q_{k+1}+\cfrac{1}{q_{k+2}+\ddots}\right)+Q_{k-1}}.$$

設$\cfrac{1}{q_{k+2}+\ddots}=\lambda\ (0<\lambda<1)$，于是

$$\alpha=\frac{P_k q_{k+1}+P_{k-1}+P_k\lambda}{Q_k q_{k+1}+Q_{k-1}+Q_k\lambda}$$

$$=\frac{P_{k+1}+P_k\lambda}{Q_{k+1}+Q_k\lambda}.$$

观察下面的情形：

---

① 如果討論的是有限連分数，那末这里δ_{k+1}是表示它的眞近似分数．事实上，这时如果δ_{k+1}与連分数的值相等，定理是显然成立的．

$$\alpha-\delta_k=\alpha-\frac{P_k}{Q_k}$$

$$=\frac{P_{k+1}+P_k\lambda}{Q_{k+1}+Q_k\lambda}-\frac{P_k}{Q_k}$$

$$=\frac{P_{k+1}Q_k-P_kQ_{k+1}}{Q_k(Q_{k+1}+Q_k\lambda)}$$

$$=\frac{(-1)^{k+1}}{Q_k(Q_{k+1}+Q_k\lambda)};$$

$$\alpha-\delta_{k+1}=\alpha-\frac{P_{k+1}}{Q_{k+1}}$$

$$=\frac{P_{k+1}+P_k\lambda}{Q_{k+1}+Q_k\lambda}-\frac{P_{k+1}}{Q_{k+1}}$$

$$=\frac{-\lambda(P_{k+1}Q_k-P_kQ_{k+1})}{Q_{k+1}(Q_{k+1}+Q_k\lambda)}$$

$$=\frac{-\lambda\cdot(-1)^{k+1}}{Q_{k+1}(Q_{k+1}+Q_k\lambda)}$$

$$=\frac{\lambda(-1)^k}{Q_{k+1}(Q_{k+1}+Q_k\lambda)}.$$

于是，

$$|\alpha-\delta_k|=\frac{1}{Q_k(Q_{k+1}+Q_k\lambda)};\quad |\alpha-\delta_{k+1}|=\frac{\lambda}{Q_{k+1}(Q_{k+1}+Q_k\lambda)};$$

因为 $0<\lambda<1$，且 $Q_{k+1}>Q_k$，因此

$$|\alpha-\delta_{k+1}|<|\alpha-\delta_k|.$$

推論 連分数的值 α 在 δ_k 和 δ_{k+1} 之間．(如果討論的是有限連分数，δ_{k+1} 应是它的眞近似分数．)

証明 由定理的証明过程中得到：

$\alpha-\delta_k$ 的值与 $(-1)^{k+1}$ 同号；

$\alpha-\delta_{k+1}$ 的值与 $(-1)^k$ 同号．

也就是説，$\alpha-\delta_k$ 的值与 $\alpha-\delta_{k+1}$ 的值异号．这就証实了断言．

因为 $\delta_{2n+1}<\delta_{2n}$，所以連分数的值 α 滿足：

$$\delta_{2n+1}<\alpha<\delta_{2n}.$$

定理 5　設連分数的值是 α，那末

$$\frac{1}{Q_k(Q_k+Q_{k+1})}<|\alpha-\delta_k|<\frac{1}{Q_kQ_{k+1}}.$$

（如果討論的是有限連分数，δ_{k+1} 就表示它的眞近似分数①.）

証明　由上面的定理的証明过程中得到：

$$|\alpha-\delta_k|=\frac{1}{Q_k(Q_{k+1}+Q_k\lambda)}.\quad(0<\lambda<1)$$

因为 $\dfrac{1}{Q_k(Q_{k+1}+Q_k\lambda)}=\dfrac{1}{Q_kQ_{k+1}+Q_k^2\lambda}<\dfrac{1}{Q_kQ_{k+1}}$，

所以 $$|\alpha-\delta_k|<\frac{1}{Q_kQ_{k+1}}.$$

又 $\dfrac{1}{Q_k(Q_{k+1}+Q_k\lambda)}=\dfrac{1}{Q_kQ_{k+1}+Q_k^2\lambda}>\dfrac{1}{Q_kQ_{k+1}+Q_k^2}$，

所以 $$|\alpha-\delta_k|>\frac{1}{Q_kQ_{k+1}+Q_k^2}.$$

这就証明了：

$$\frac{1}{Q_k(Q_{k+1}+Q_k)}<|\alpha-\delta_k|<\frac{1}{Q_kQ_{k+1}}.$$

例　將圓周率 $\pi=3.14159\cdots\cdots$ 化作連分数，用近似分数表示它，并求出对应的誤差范圍.

π 所对应的連分数，經計算后，結果如下：

---

①　如果討論的是有限連分数，而 $\delta_{k+1}=\alpha$. 这样

$$|\alpha-\delta_k|=|\delta_{k+1}-\delta_k|=\frac{1}{Q_kQ_{k+1}}.$$

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}}}.$$

由 $\delta_1 = \frac{3}{1}$，$\delta_2 = \frac{22}{7}$，可求得：

$$\delta_3 = \frac{22 \cdot 15 + 3}{7 \cdot 15 + 1} = \frac{333}{106};$$

$$\delta_4 = \frac{333 \cdot 1 + 22}{106 \cdot 1 + 7} = \frac{355}{113};$$

$$\delta_5 = \frac{355 \cdot 292 + 333}{113 \cdot 292 + 106} = \frac{103993}{33102};$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots.$$

（很明显，近似分数 δ_2 和 δ_4 分别是祖冲之圓周率的疏率及密率。）

我們計算一下用 $\delta_2 = \frac{22}{7}$，$\delta_4 = \frac{355}{113}$ 表示 π 时的誤差范圍：

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{7 \cdot 106} = \frac{1}{742} < \frac{1}{500};$$

$$\left|\pi - \frac{355}{133}\right| < \frac{1}{133 \cdot 33102} = \frac{1}{4402566} < \frac{1}{10^6}.$$

定理 6 如果既約分数 $\frac{a}{b}$ 比近似分数 $\delta_k\left(\delta_k = \frac{P_k}{Q_k}\right)$ 更接近于連分数的值 α，那末 $b > Q_k$。

証明 因为 δ_k 比 δ_{k-1} 接近于 α，由条件知 $\frac{a}{b}$ 比 δ_k 接近于 α，所以 $\frac{a}{b}$ 比 δ_{k-1} 更接近于 α。而 $\frac{a}{b}$ 在 δ_k 和 δ_{k-1} 之間（因为 α 在 δ_k 和 δ_{k-1} 之

間，而$\frac{a}{b}$比 δ_k 及 δ_{k-1} 更接近于 α)。

也就是 $$\left|\frac{a}{b}-\delta_{k-1}\right|<\left|\delta_k-\delta_{k-1}\right|.$$

于是， $$\left|\frac{aQ_{k-1}-bP_{k-1}}{bQ_{k-1}}\right|<\left|\frac{(-1)^k}{Q_kQ_{k-1}}\right|.$$

因为 b 和 Q_{k-1} 都大于零,就得到

$$\frac{|aQ_{k-1}-bP_{k-1}|}{bQ_{k-1}}<\frac{1}{Q_kQ_{k-1}}.$$

不等式两边同乘以 bQ_{k-1}，得:

$$|aQ_{k-1}-bP_{k-1}|<\frac{b}{Q_k}.$$

显然，$|aQ_{k-1}-bP_{k-1}|$ 不是正整数就是零．但是 $aQ_{k-1}-bP_{k-1}$ 不可能等于零．因为如果 $aQ_{k-1}-bP_{k-1}=0$，那末 $\frac{a}{b}-\frac{P_{k-1}}{Q_{k-1}}=0$．这就与"$\frac{a}{b}$ 比 δ_{k-1} 更接近于 α"矛盾．

既然 $|aQ_{k-1}-bP_{k-1}|$ 应是正整数,于是至少应有 $\frac{b}{Q_k}>1$.

因此 $b>Q_k$.

这条定理也可以表达如下:

近似分数 $\delta_k=\frac{P_k}{Q_k}$ 是一切分母不大于 Q_k 的分数中最接近于連分数的值．

§4 連分数的应用

1．求平方根

我們先用实数化为連分数的方法,来求平方根．

例 求 $\sqrt{41}$ 的近似值．

因为 $[\sqrt{41}]=6$,

所以 $$\sqrt{41}=6+(\sqrt{41}-6)$$
$$=6+\frac{1}{\frac{1}{\sqrt{41}-6}}=6+\frac{1}{\frac{\sqrt{41}+6}{5}}. \quad (1)$$

又 $\left[\frac{\sqrt{41}+6}{5}\right]=2$,

所以 $$\frac{\sqrt{41}+6}{5}=2+\frac{\sqrt{41}-4}{5}$$
$$=2+\frac{1}{\frac{5}{\sqrt{41}-4}}=2+\frac{1}{\frac{\sqrt{41}+4}{5}}. \quad (2)$$

又 $\left[\frac{\sqrt{41}+4}{5}\right]=2$,

所以 $$\frac{\sqrt{41}+4}{5}=2+\frac{\sqrt{41}-6}{5}$$
$$=2+\frac{1}{\frac{5}{\sqrt{41}-6}}=2+\frac{1}{\sqrt{41}+6}. \quad (3)$$

又 $[\sqrt{41}+6]=12$,
$$\sqrt{41}+6=12+(\sqrt{41}-6)$$
$$=12+\frac{1}{\frac{1}{\sqrt{41}-6}}=12+\frac{1}{\frac{\sqrt{41}+6}{5}}. \quad (4)$$

由(1)、(2)、(3)、(4)得到

$$\sqrt{41}=6+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{12+\cfrac{\sqrt{41}+6}{5}}}}.$$

由于(4)的最后的分式与(1)的最后的分式相同，可知：如果繼續写出$\sqrt{41}$ 对应的連分数的部分分母，必与前面的部分分母构成循环．

$$\sqrt{41}=6+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{12+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{12+\ddots}}}}}}$$

根据前面的方法，可求出該連分数的近似值．例如，

$$\delta_3=\frac{32}{5},\quad \delta_4=\frac{397}{62},\quad \delta_5=\frac{826}{129},\quad \cdots\cdots,$$

因此得：

$$\sqrt{41}\approx\frac{32}{5},\quad \left(\text{誤差 } \alpha<\frac{1}{310}\right)$$

$$\sqrt{41}\approx\frac{397}{62},\quad \left(\text{誤差 } \alpha<\frac{1}{62\cdot129}\right)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

注 对于一个非完全平方的整数，它的平方根所对应的連分数必是循环的(部分分母是循环地重复着的)．且从第二个部分分母开始循环．不仅如此，对于一般的二次不尽根数，如 $a_1+a_2\sqrt{b}$ (a_1、a_2 都是不等于零的有理数，b 是非完全平方的正整数）所对应的連分数，也一定是循环的．反过来，循环連分数的值一定是二次不尽根数．(上面的論断，証明較繁杂，这里不准备介紹.)

上面所述的平方根的求法，計算較繁，我們找到了$\sqrt{N}$ 近似值的一般求法：

設
$$N=a^2+b.\qquad (a>0)$$

于是

$$\sqrt{N}=a+(\sqrt{N}-a)$$

$$=a+\frac{N-a^2}{a+\sqrt{N}}$$

$$=a+\frac{b}{a+\sqrt{N}}.$$

显然，在所得到的分式中的 $\sqrt{N}$，也可以用 $a+\dfrac{b}{a+\sqrt{N}}$ 代替，这样繼續下去，就得到：

$$\sqrt{N}=a+\cfrac{b}{a+a+\cfrac{b}{a+\sqrt{N}}}$$

$$=\cdots\cdots\cdots\cdots\cdots\cdots$$

$$=a+\cfrac{b}{2a+\cfrac{b}{2a+\ddots}}.$$

随着不同的精确度的要求，可取

$$\sqrt{N}\approx a+\frac{b}{2a}, \tag{1}$$

$$\sqrt{N}\approx a+\cfrac{b}{2a+\cfrac{b}{2a}}=a+\frac{2ab}{4a^2+b}, \tag{2}$$

$$\sqrt{N}\approx a+\cfrac{b}{2a+\cfrac{b}{2a+\cfrac{b}{2a}}}=a+\frac{4a^2b+b^2}{8a^3+4ab}. \tag{3}$$

等等.

例1 求 $\sqrt{41}$ 的近似值.

因为 $41=6^2+5$,

由公式(1)，得： $\sqrt{41}\approx 6+\dfrac{5}{12}\approx 6.4$;

由公式(2)，得： $\sqrt{41}\approx 6+\dfrac{60}{149}\approx 6.403$.

例 2 求 $\sqrt{105}$ 的近似值.

因为 $105=10^2+5$,

由公式 (1), 得: $\sqrt{105}\approx 10+\frac{5}{20}=10.25$;

由公式 (2), 得: $\sqrt{105}\approx 10+\frac{100}{405}\approx 10.247$.

(上述平方根近似值的求法,缺点在于不容易估計近似值的誤差范圍.)

2. 求对数值

对数值是可以用初等方法解决的，这里举例說明应用連分数的知識来求对数值.

例 求以 10 为底的 2 的对数.

很明显, $0<\log_{10}2<1$.

設 $\log_{10}2=\frac{1}{x}$, 即 $10^{\frac{1}{x}}=2$, 或 $2^x=10$.

不难看出 $3<x<4$.

設 $x=3+\frac{1}{x_1}$, 于是

$$2^{3+\frac{1}{x_1}}=10.$$

也就是 $8\cdot 2^{\frac{1}{x_1}}=10$, $2^{\frac{1}{x_1}}=\frac{5}{4}$. 于是

$$\left(\frac{5}{4}\right)^{x_1}=2.$$

从观察可知: $3<x_1<4$.

設 $x_1=3+\frac{1}{x_2}$, 于是

$$\left(\frac{5}{4}\right)^{3+\frac{1}{x_2}}=2.$$

也就是 $$\frac{128}{125}=\left(\frac{5}{4}\right)^{\frac{1}{x_2}}. \qquad \left(\frac{128}{125}\right)^{x_2}=\frac{5}{4}.$$

可以知道: $$9<x_2<10.$$

設 $x_2=9+\frac{1}{x_3}$, 再按照上面作过的步驟重复做去. 这样繼續做下去的結果就得到下面的等式:

$$x_3=2+\frac{1}{x_4},$$

$$x_4=2+\frac{1}{x_5},$$

$$x_5=4+\frac{1}{x_6},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots.$$

于是,对于 $\log_{10}2$,可以写成連分数的形式:

$$\log_{10}2=\frac{1}{x}=\frac{1}{3+\frac{1}{x_1}}=\frac{1}{3+\frac{1}{3+\frac{1}{x_2}}}$$

$$=\cdots\cdots\cdots\cdots\cdots$$

$$=\frac{1}{3+\frac{1}{3+\frac{1}{9+\frac{1}{2+\frac{1}{2+\frac{1}{4+\ddots}}}}}}.$$

容易求得:

$$\delta_1=0, \quad \delta_2=\frac{1}{3}, \quad \delta_3=\frac{3}{10}, \quad \delta_4=\frac{28}{93}, \quad \delta_5=\frac{58}{196},$$

$$\delta_6=\frac{146}{485}, \quad \delta_7=\frac{643}{2136}, \quad \delta_8=\frac{2718}{9029}, \quad \cdots\cdots\cdots.$$

于是，如果取 $\log_{10}2\approx\frac{146}{485}$ $\left(\text{誤差}\ \alpha<\frac{1}{485\cdot2136}<\frac{1}{10^6}\right)$，

把 $\frac{146}{485}$ 化作十进小数：$\frac{146}{485}=0.3010309\cdots\cdots$，

因此 $\log_{10}2\approx0.301030$.

如果取 $\log_{10}2\approx\frac{643}{2136}$ $\left(\text{誤差}\ \alpha<\frac{1}{2136\cdot9029}<\frac{1}{10^7}\right)$，

把 $\frac{643}{2136}$ 化作十进小数，于是得：

$$\log_{10}2\approx0.3010299.$$

应該指出，虽然可以用連分数来求对数的近似值，但由于計算过程的浩繁，所以这个方法就显得很不方便．当然，現在計算对数値已具备了相当完善的工具．

3．求整系数方程 $ax+by=c$ 的整数解．

分成两种情况来解决：

(1) 方程 $ax+by=c$.

[这里 a 和 b 都大于 0，且 $(a,b)=1$.]

把 $\frac{a}{b}$ 化成連分数（当然一定是有限連分数），并設末一个近似分数为 δ_n $\left(\text{当然，}\ \delta_n=\frac{P_n}{Q_n}=\frac{a}{b}\right)$.

由定理 2，得

$$aQ_{n-1}-bP_{n-1}=(-1)^n.$$

也就是 $$aQ_{n-1}+b(-P_{n-1})=(-1)^n.$$

等式两边各乘以 $(-1)^n\cdot c$，得：

$$a[(-1)^n\cdot c\cdot Q_{n-1}]+b[(-1)^{n+1}\cdot c\cdot P_{n-1}]=c.$$

因此方程 $ax+by=c$ 的一組特殊整数解是：

$$\begin{cases}x_0=(-1)^n cQ_{n-1},\\ y_0=(-1)^{n+1}cP_{n-1}.\end{cases}$$

于是它的一般的整数解公式是：

$$\begin{cases} x=(-1)^{n}cQ_{n-1}-bt, \\ y=(-1)^{n+1}cP_{n-1}+at. \end{cases} \quad (t=0、\pm1、\pm2、\cdots\cdots)$$

(2) 方程 $ax+by=c$。

［这里 $a>0$，$b<0$，且 $(a, |b|)=1$］

把 $\frac{a}{|b|}$ 化成連分数，并設末一个近似分数为 δ_n。同样地，

$$aQ_{n-1}-|b|P_{n-1}=(-1)^{n}.$$

也就是

$$aQ_{n-1}+bP_{n-1}=(-1)^{n}.$$

等式两边各乘以 $(-1)^{n}c$，得：

$$a[(-1)^{n}cQ_{n-1}]+b[(-1)^{n}cP_{n-1}]=c.$$

因此上述方程的一組特殊整数解是：

$$\begin{cases} x_0=(-1)^{n}cQ_{n-1}, \\ y_0=(-1)^{n}cP_{n-1}. \end{cases}$$

于是它的一般的整数解公式是：

$$\begin{cases} x=(-1)^{n}cQ_{n-1}-bt, \\ y=(-1)^{n}cP_{n-1}+at. \end{cases} \quad (t=0、\pm1、\pm2、\cdots\cdots)$$

例 1 求方程 $43x+15y=8$ 的整数解。

先把 $\frac{43}{15}$ 化成連分数，得：

$$\frac{43}{15}=2+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{2}}}.$$

很明显，δ_{n-1} 是 δ_3。而近似分数 $\delta_3=\frac{20}{7}$，因此一組特殊的整数解是：

$$\begin{cases} x_0=(-1)^{4}\cdot8\cdot7=56, \\ y_0=(-1)^{5}\cdot8\cdot20=-160. \end{cases}$$

一般整数解的公式是：

$$\begin{cases} x=56-15t, \\ y=-160+43t. \end{cases} \quad (t=0、\pm1、\pm2、\cdots\cdots)$$

例 2 求方程 $7x-19y=5$ 的整数解.

把 $\frac{7}{19}$ 化成連分数，得：

$$\frac{7}{19}=\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{2}}}}.$$

显然，δ_{n-1} 是 δ_4，由 $\delta_1=0$，$\delta_2=\frac{1}{2}$，$\delta_3=\frac{1}{3}$，得：

$$\delta_4=\frac{2\cdot1+1}{2\cdot3+2}=\frac{3}{8}.$$

所以一組特殊的整数解是：

$$\begin{cases} x_0=(-1)^5\cdot5\cdot8=-40, \\ y_0=(-1)^5\cdot5\cdot3=-15. \end{cases}$$

一般整数解的公式是：

$$\begin{cases} x=-40+19t, \\ y=-15+7t. \end{cases} \quad (t=0、\pm1、\pm2、\cdots\cdots)$$

由上，可作如次的結論：

方程 $ax+by=c$，如果$(|a|, |b|)=1$，那末一定有整数解．或方程 $ax+by=c$，如果 $c \vdots (|a|, |b|)$，那末一定有整数解.

早在18世紀，数学家拉格兰日曾用連分数来求代数方程的根，因为要涉及到高等代数中的一些知識，因此这里不作介紹了.

第九章　中国剩余定理

这一章的内容，实际上就是一次同余組的解法．而这里比較詳細地介紹的，是我們祖国古代的数学家在这个問題上的貢献．这些貢献得到了很高的評价，外国的書籍上把这个法則叫做中国剩余定理．

§1　中国剩余定理

在我国古代数学書籍"孙子算經"卷下，列有这样一个問題，以及它的解答：

"今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，問物几何．

答曰：二十三．

术曰：三三数之剩二，置一百四十；五五数之剩三，置六十三；七七数之剩二，置三十；幷之，得二百三十三，以二百十一减之即得．"

書中接着就对这类問題給出了一般解法：

"凡三三数之剩一，則置七十；五五数之剩一，則置二十一；七七数之剩一，則置十五；一百六以上，以一百五减之即得．"

上述，即表明了下面的同余式組的解法：

$$\begin{cases} x \equiv R_1 \pmod{3}, \\ x \equiv R_2 \pmod{5}, \\ x \equiv R_3 \pmod{7}. \end{cases} \tag{I}$$

这里模数 3、5、7 是两两互質的，所以

$$[3,\ 5,\ 7]=3\cdot5\cdot7=3\cdot35=5\cdot21=7\cdot15\text{（乘积都等于 105）}.$$

且

$$35\cdot2\equiv1 \pmod{3},$$

$$21\cdot1\equiv1 \pmod{5},$$

$$15\cdot1\equiv1 \pmod{7}.$$

这样，显然可得：

$$70R_1 \equiv R_1 \pmod{3},$$
$$21R_2 \equiv R_2 \pmod{5},$$
$$15R_3 \equiv R_3 \pmod{7}.$$

于是，

$$70R_1+21R_2+15R_3 \equiv 70R_1 \equiv R_1 \pmod{3},$$
$$70R_1+21R_2+15R_3 \equiv 21R_2 \equiv R_2 \pmod{5},$$
$$70R_1+21R_2+15R_3 \equiv 15R_3 \equiv R_3 \pmod{7}.$$

因此同余式組(I)的解是滿足下面同余式組的整数值 x：

$$\begin{cases} x \equiv 70R_1+21R_2+15R_3 \pmod{3}, \\ x \equiv 70R_1+21R_2+15R_3 \pmod{5}, \\ x \equiv 70R_1+21R_2+15R_3 \pmod{7}. \end{cases} \qquad \text{(II)}$$

因为$[3,5,7]=105$，因此同余式組(II)与下面的同余式是同解的：

$$x \equiv 70R_1+21R_2+15R_3 \pmod{105}. \qquad \text{(III)}$$

也就是說，同余式組(I)的解是同余式(III)的解.

如“孙子算經”原題：$R_1=2$，$R_2=3$，$R_3=2$；那末

$$x \equiv 140+63+30 \equiv 23 \pmod{105}.$$

因此适合該問題的非負最小值是 23.

下面来研究較一般的定理.

定理 設有同余式組：

$$\begin{cases} x \equiv R_1 \pmod{A}, \\ x \equiv R_2 \pmod{B}, \\ x \equiv R_3 \pmod{C}. \end{cases} \qquad \text{(I)}$$

（这里 A、B、C 是两两互質的）

如果整数 α、β、γ① 滿足下面三式：

$$\alpha BC \equiv 1 \pmod{A},$$
$$\beta AC \equiv 1 \pmod{B},$$
$$\gamma AB \equiv 1 \pmod{C}.$$

① 整数 α、β、γ 如何找到，讀了 §2 就可解决.

那末(I)的解是:

$$x\equiv \alpha BCR_1+\beta ACR_2+\gamma ABR_3 \pmod{ABC}.$$

証明

因为 $\alpha BC\equiv 1 \pmod{A}$，所以 $\alpha BCR_1\equiv R_1 \pmod{A}$.

又 $\beta AC\equiv 1 \pmod{B}$，所以 $\beta ACR_2\equiv R_2 \pmod{B}$.

又 $\gamma AB\equiv 1 \pmod{C}$，所以 $\gamma ABR_3\equiv R_3 \pmod{C}$.

这样:

$$\alpha BCR_1+\beta ACR_2+\gamma ABR_3\equiv \alpha BCR_1\equiv R_1 \pmod{A},$$
$$\alpha BCR_1+\beta ACR_2+\gamma ABR_3\equiv \beta ACR_2\equiv R_2 \pmod{B},$$
$$\alpha BCR_1+\beta ACR_2+\gamma ABR_3\equiv \gamma ABR_3\equiv R_3 \pmod{C}.$$

因此(I)的解是满足下面同余式組的整数值 x:

$$\begin{cases} x\equiv \alpha BCR_1+\beta ACR_2+\gamma ABR_3 \pmod{A}, \\ x\equiv \alpha BCR_1+\beta ACR_2+\gamma ABR_3 \pmod{B}, \\ x\equiv \alpha BCR_1+\beta ACR_2+\gamma ABR_3 \pmod{C}. \end{cases} \qquad \text{(II)}$$

因为 A、B、C 两两互質，于是 $[A, B, C]=ABC$. 所以同余式組(II)与下面的同余式是同解的:

$$x\equiv \alpha BCR_1+\beta ACR_2+\gamma ABR_3 \pmod{ABC}.$$

上式也就是同余式組(I)的解.

对更加一般的情形，有下面的定理:

如果

$$\begin{cases} x\equiv R_1 \pmod{m_1}, \\ x\equiv R_2 \pmod{m_2}, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x\equiv R_k \pmod{m_k}. \end{cases} \qquad \text{(I)}$$

（这里 m_1、m_2、……、m_k 是两两互質的）

設 $m_1m_2\cdots\cdots m_k=M_sm_s$ $(s=1、2、\cdots\cdots、k)$.

又整数 N_s，满足下式:

$$M_sN_s\equiv 1 \pmod{m_s},$$

那末同余式組(I)的解是:

$$x \equiv M_1N_1R_1 + M_2N_2R_2 + \cdots\cdots + M_kN_kR_k \pmod{m_1m_2\cdots\cdots m_k}.$$

它的証明与上面介紹的定理的証明一样,因此省略了.

例 1 解同余式組:

$$\begin{cases} x \equiv 3 \pmod{5}, \\ x \equiv 5 \pmod{9}. \end{cases}$$

因为

$$(-1)\cdot 9 \equiv 1 \pmod{5},$$
$$2\cdot 5 \equiv 1 \pmod{9},$$

所以同余式組的解是:

$$x \equiv (-1)\cdot 9\cdot 3 + 2\cdot 5\cdot 5 = 23 \pmod{45}.$$

例 2 解同余式組:

$$\begin{cases} x \equiv 1 \pmod{7}, \\ x \equiv 3 \pmod{5}, \\ x = 5 \pmod{9}. \end{cases}$$

因为

$$(-2)\cdot 5\cdot 9 \equiv 1 \pmod{7},$$
$$2\cdot 7\cdot 9 \equiv 1 \pmod{5},$$
$$(-1)\cdot 7\cdot 5 \equiv 1 \pmod{9}.$$

所以同余式組的解是:

$$x \equiv (-2)\cdot 5\cdot 9 + 2\cdot 7\cdot 9\cdot 3 + (-1)\cdot 7\cdot 5\cdot 5$$
$$= 113 \pmod{315}.$$

上面所討論的只是当模数为两两互质时的情形. 下面将討論到当模数不是两两互质时的情形.

例如問題: 設 $A = ad^p$, $B = bd^q$, $C = cd^r$,

(这里 a、b、c、d 两两互质,又不妨假定 q、r 不比 p 大.)

解同余式組:

$$\begin{cases} x \equiv R_1 \pmod{A}, \\ x \equiv R_2 \pmod{B}, \\ x \equiv R_3 \pmod{C}. \end{cases} \tag{I}$$

很明显，上面的同余式組与下面的同余式組是同解的：

$$\left\{\begin{array}{ll} x\equiv R_1 \pmod{A}, & (1) \\ x\equiv R_2 \pmod{b}, & (2) \\ x\equiv R_2 \pmod{d^q}, & (3) \\ x\equiv R_3 \pmod{c}, & (4) \\ x\equiv R_3 \pmod{d^r}. & (5) \end{array}\right. \qquad \text{(II)}$$

因为 d^q、d^r 是 A 的約数，所以从(1)式就得到：

$$x\equiv R_1 \pmod{d^q}, \qquad x\equiv R_1 \pmod{d^r}.$$

于是，
$$R_1\equiv R_2 \pmod{d^q}, \quad R_1\equiv R_3 \pmod{d^r}.$$

这就說明了满足(1)的 x 值，一定满足于(3)与(5)．于是同余式組(II)与下面的同余式組是同解的：

$$\left\{\begin{array}{l} x\equiv R_1 \pmod{A}, \\ x\equiv R_2 \pmod{b}, \\ x\equiv R_3 \pmod{c}. \end{array}\right. \qquad \text{(III)}$$

这里，显然 A、b、c 是两两互质的．因此解同余式組(III)的工作就归結到前面去了．

例 1　解同余式組：

$$\left\{\begin{array}{l} x\equiv 3 \pmod{25}, \\ x\equiv 8 \pmod{20}. \end{array}\right.$$

因为 $20=4\cdot 5$，而且 $25 \vdots 5$，同时 $8\equiv 3 \pmod{5}$，所以上面的同余式組与下面的同余式組同解：

$$\left\{\begin{array}{l} x\equiv 3 \pmod{25}, \\ x\equiv 8 \pmod{4}. \end{array}\right.$$

又 $(-6)\cdot 4\equiv 1 \pmod{25}$，$1\cdot 25\equiv 1 \pmod{8}$，因此同余式組的解是：

$$x\equiv(-6)\cdot 4\cdot 3+25\cdot 8\equiv 28 \pmod{100}.$$

例 2　解同余式組：

$$\begin{cases} x \equiv 8 \pmod{15}, \\ x \equiv 5 \pmod{18}, \\ x \equiv 13 \pmod{25}. \end{cases}$$

这里$(18, 25)=1$，而$15=3\cdot5$，可以看到：$18 \vdots 3$，且$8\equiv5 \pmod 3$；$25 \vdots 5$，且$8\equiv13 \pmod 5$．所以上面的同余式組与下面的同解：

$$\begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 13 \pmod{25}. \end{cases}$$

而这是我們可以解决的．

例 3　解同余式組：

$$\begin{cases} x \equiv 13 \pmod{54}, \\ x \equiv 17 \pmod{45}, \\ x \equiv 5 \pmod{21}. \end{cases}$$

因为$54=2\cdot3^3$，$45=5\cdot3^2$，$21=3\cdot7$，容易看到，21 的因数 3 是 54 的約数，然而$13 \not\equiv 5 \pmod 3$．上面的事实就指出了这个同余式組无解．

§2 求 乘 率

1．大衍求一术

"A、B 为互質的两整数，求出一整数 α，，使滿足同余式

$$\alpha B \equiv 1 \pmod A."$$

解决上面的問題，也即完善地解决了孙子問題．

我国宋代数学家秦九韶所著"数学九章"(1247)，其中論述的"大衍求一术"就是解决上面的問題的一般方法．到了清代，数学家黃宗宪在所著"求一术通解"(1896)里又把它簡化．下面作一簡单介紹．

古代数学家管数 A 叫定母，B 叫衍数，滿足条件 $\alpha B\equiv1 \pmod A$ 的整数 α，叫做乘率．

下面是黃宗宪在"求一术通解"里的求乘率的方法：

"列定母于右行，列衍数于左行〔左角上預寄一数〕輾轉累減〔凡定

母与衍数輾轉累減，則其上所寄数，必輾轉累加，至衍数余一即止，視左角上之寄数为乘率。”

“按两数相减，必以少数为法，多数为实①。其法上无寄数者，不論减若干次，减余数上仍以一为寄数；其实上无寄数者，减余数上，以所减次数为寄数；其法上实上俱有寄数者，視累减若干次，以法上寄数亦累加若干次于实上寄数中，即得减余数上之寄数矣！”

我們先从具体例子来解释这个法則，然后再一般的加以証明。

例 1 已知衍数为 35，定母为 3，求乘率。

按上述法則，可以写成：

寄数	衍数	定母	寄数
1	35	3	
	33	2	
1	2	1	1
	1		
2	1		

因此乘率为 2，即 $2 \cdot 35 \equiv 1 \pmod 3$。

因定母 3 比衍数 35 小，所以由 35 中累减 3（共减 11 次），得余数为 2。按照法則所說，法上无寄数，不論减若干次，所得的余数（这里是 2）仍以 1 为寄数。所以在余数 2 的左角寄上数 1。接着从 3 中累减 2（仅减一次）得余数为 1。按照法則所說，实上无寄数，以所减次数（这里所减次数为 1）为余数的寄数。所以在余数 1 的右角寄上数 1。再从 2 中累减 1，因为要使衍数一列保留余数 1，所以仅从 2 中减去一次 1，得余数 1，按照法則所說，法实都有寄数，視累减若干次（这里仅一次）以法上的寄数（这里是 1）亦累加若干次于实上的寄数（这里也是 1），得到的数即是余数的寄数。显然，最后的余数 1 的寄数为 $1 \cdot 1+1=2$。

例 2 已知衍数为 45，定母为 8，求乘率。

① “实”指的是被减数；“法”指的是减数。

寄数	衍数	定母	寄数
1	45 40	8 5	
1	5 3	3 2	1
2	2 1	1	3
5	1		

由上知,乘率为 5 .也就是 $5 \cdot 45 \equiv 1 \pmod 8$。

例 3 已知衍数为 25 ,定母为 18 ,求乘率.

寄数	衍数	定母	寄数
1	25 18	18 14	
1	7 4	4 3	2
3	3 2	1	5
13	1		

由上知,乘率为 13 .也就是 $13 \cdot 25 \equiv 1 \pmod{18}$。

下面我們用一般的算式来写出这个法則:

設 B 为衍数, A 为定母,由法則知:

寄　　数	衍　数	定　母	寄　　数
1	B Aq_1	A r_1q_2	
$k_1=1$	r_1 r_2q_3	r_2 r_3q_4	$k_2=q_2$
$k_3=k_2q_3+k_1$	r_3	r_4	$k_4=k_3q_4+k_2$
…………………	………	………	…………………
$k_{n-2}=k_{n-3}q_{n-2}+k_{n-4}$	r_{n-2} $r_{n-1}q_n$	r_{n-1}	$k_{n-1}=k_{n-2}q_{n-1}+k_{n-3}$
$k_n=k_{n-1}q_n+k_{n-2}$	$r_n(=1)$		

于是得到乘率为 k_n（事实上，满足 $\alpha\equiv k_n \pmod{A}$ 的一切 α 的值，都可作为乘率）。

（顺便可知：n 为奇数，因为 r_n 留在左边.）

上面的安排，也就是下面的意思：

$B=Aq_1+r_1 \quad (1<r_1<A)$	$k_1=1$
$A=r_1q_2+r_2 \quad (1<r_2<r_1)$	$k_2=q_2$
$r_1=r_2q_3+r_3 \quad (1<r_3<r_2)$	$k_3=k_2q_3+k_1$
$r_2=r_3q_4+r_4 \quad (1<r_4<r_3)$	$k_4=k_3q_4+k_2$
…………………………………	…………………
$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}(1<r_{n-1}<r_{n-2})$	$k_{n-1}=k_{n-2}q_{n-1}+k_{n-3}$
$r_{n-2}=r_{n-1}q_n+r_n \quad (r_n=1)$	$k_n=k_{n-1}q_n+k_{n-2}$

（n 为奇数）

至于为什么 k_n 即是乘率，下面进行証明.

由上可知：

$$r_1=B-Aq_1$$
$$=k_1B-t_1A. \qquad t_1=q_1.$$
$$r_2=A-r_1q_2$$
$$=A-(k_1B-t_1A)q_2$$
$$=A+t_1q_2A-k_1q_2B$$
$$=(t_1q_2+1)A-q_2B$$
$$=t_2A-k_2B. \qquad t_2=t_1q_2+1.$$
$$r_3=r_1-r_2q_3$$
$$=(k_1B-t_1A)-(t_2A-k_2B)q_3$$
$$=(k_2q_3+k_1)B-(t_2q_3+t_1)A$$
$$=k_3B-t_3A. \qquad t_3=t_2q_3+t_1.$$

………………………………… …………………

$$r_s=(t_sA-k_sB)\cdot(-1)^s \qquad t_s=t_{s-1}q_s+t_{s-2}.$$

………………………………… …………………

因为n为奇数，所以

$$r_n=k_nB-t_nA. \qquad t_n=t_{n-1}q_n+t_{n-2}.$$

因为$r_n=1$，所以$k_nB=t_nA+1$. 因此

$$k_nB\equiv 1\ (\mathrm{mod}\ A).$$

求乘率的問題，一般地得到了解决．也就是說，孙子的問題得到了一般的解决．

除此以外，在黃宗宪著“求一术通解”中另有利用“反乘率”来解孙子的問題，方法也很巧妙，現簡略介紹如下．

如果要解同余式組：

$$\begin{cases} x\equiv R_1\ (\mathrm{mod}\ m_1), \\ x\equiv R_2\ (\mathrm{mod}\ m_2), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x\equiv R_k\ (\mathrm{mod}\ m_k). \end{cases} \tag{I}$$

(m_1、m_2、……、m_k两两互质)

設R'_i ($i=1$、2、……、k)$\geqslant 0$，且$-R'_i\equiv R_i\ (\mathrm{mod}\ m_i)$，那末同余式組(I)与下面的同余式組是显然同解的：

$$\begin{cases} x\equiv -R'_1\ (\mathrm{mod}\ m_1), \\ x\equiv -R'_2\ (\mathrm{mod}\ m_2), \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x\equiv -R'_k\ (\mathrm{mod}\ m_k). \end{cases}$$

設$m_1m_2\cdots\cdots m_k=M_sm_s$ ($s=1$、2、……、k)，又整数N'_s满足同余式：

$$M_sN'_s\equiv -1\ (\mathrm{mod}\ m_s),$$

那末同余式組(I)的解是：

$$x\equiv M_1N'_1R'_1+M_2N'_2R'_2+\cdots\cdots+M_kN'_kR'_k\ (\mathrm{mod}\ m_1m_2\cdots\cdots m_k).$$

(定理的証明与§1定理的証明相仿，这里从略.)

定理中的N'_s，就是反乘率．至于如何求反乘率，与求乘率的法則沒有多大区別．照求乘率的法則所說：“列定母于右行，列衍数于左行，

輾轉累减，至衍数余一为止，視左角之寄数为乘率."而求反乘率，只是輾轉累减至定母余一为止，視右角之寄数为反乘率．其他如寄数的求法，均与求乘率的完全相同．

例 1 設衍数为 35，定母为 3，求反乘率．

按照法則：

寄数	衍数	定母	寄数
1	35	3	
	33	2	
1	2	1	1

可知，反乘率为 1．就是 $1\cdot 35\equiv -1 \pmod 3$．

例 2 設衍数为 45，定母为 8，求反乘率．

按照法則：

寄数	衍数	定母	寄数
1	45	8	
	40	5	
1	5	3	1
	3	2	
2	2	1	3

可知，反乘率为 3．就是 $3\cdot 45\equiv -1 \pmod 8$．

至于为什么这个求反乘率的方法是正确的，我們来証明一下．

設 B 为衍数，A 为定母，根据求反乘率的法則，可知：

$$
\begin{array}{ll|l}
B=Aq_1+r_1 & (1<r_1<A) & k_1=1 \\
A=r_1q_2+r_2 & (1<r_2<r_1) & k_2=q_2 \\
r_1=r_2q_3+r_3 & (1<r_3<r_2) & k_3=k_2q_3+k_1 \\
\cdots\cdots & & \cdots\cdots \\
r_{n-3}=r_{n-2}q_{n-1}+r_{n-1} & (1\leqslant r_{n-1}<r_{n-2}) & k_{n-1}=k_{n-2}q_{n-1}+k_{n-3} \\
r_{n-2}=r_{n-1}q_n+r_n & (r_n=1) & k_n=k_{n-1}q_n+k_{n-2}
\end{array}
$$

（这里 n 应是偶数，因为 r_n 留在定母一列中．）k_n 就是反乘率．这可以仿照前面"求乘率法則的証明"而获得証明：

由前面知道：

$$r_s=(t_sA-k_sB)\cdot(-1)^s,\quad t_s=t_{s-1}q_s+t_{s-2}.$$

因为 n 是偶数，所以得： $r_n=t_nA-k_nB$.

又因为 $r_n=1$，于是 $k_nB=-1+t_nA$.

所以 $$k_nB\equiv-1\ (\mathrm{mod}\ A).$$

注 設 B 为衍数，A 为定母，那末乘率（或反乘率）**存在的充分而且必要条件是**：A 与 B 互质.

理由很簡单，留給讀者解决.

2. 用連分数求乘率

	B Aq_1	A r_1q_2	q_1
q_2	r_1 r_2q_3	r_2 r_3q_4	q_3
q_4	r_3 ·········	r_4 ·········	
q_{n-1}	r_{n-2} $r_{n-1}q_n$	r_{n-1} r_nq_{n+1}	q_n
q_{n+1}	r_n	$r_{n+1}=0$	

設 A、B 为两互质的整数，求出一整数 α，使满足同余式：

$$\alpha B\equiv1\ (\mathrm{mod}\ A).$$

我們用連分数来表示分数$\frac{B}{A}$. 由上一章知道，把普通分数化成連分数，先应輾轉相除（如上），以求得部分分母，于是得到：

$$\frac{B}{A}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_n+\cfrac{1}{q_{n+1}}}}}.$$

观察近似分数：

$$\frac{P_n}{Q_n} \text{ 与 } \frac{P_{n+1}}{Q_{n+1}} \left(\frac{P_{n+1}}{Q_{n+1}}=\frac{B}{A}\right),$$

得到：

$$\frac{B}{A}-\frac{P_n}{Q_n}=\frac{(-1)^{n+1}}{AQ_n}.$$

也就是 $BQ_n=(-1)^{n+1}+AP_n$.

因此 $BQ_n\equiv(-1)^{n+1} \pmod{A}$,

$$B[(-1)^{n+1}Q_n]\equiv 1 \pmod{A}.$$

所以 $\alpha\equiv(-1)^{n+1}Q_n \pmod{A}$.

Q_n 就是连分数的末了第二个近似分数的分母．根据连分数近似分数的分子分母构成法则可以求出 Q_n 的．

例1 求 α，使 $107\alpha\equiv 1 \pmod{37}$.

$$\frac{107}{37}=2+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{4}}},$$

这里 $n+1=4$.

因为 $Q_1=1$，$Q_2=1$，所以 $Q_3=1\cdot 8+1=9$，于是

$$\alpha\equiv(-1)^4\cdot 9=9 \pmod{37}.$$

例2 求 α，使 $45\alpha\equiv 1 \pmod{8}$.

$$\frac{45}{8}=5+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}},$$

这里 $n+1=5$.

因为 $Q_1=1$，$Q_2=1$，所以 $Q_3=1\cdot 1+1=2$，于是 $Q_4=2\cdot 1+1=3$.

因此

$$\alpha\equiv(-1)^5\cdot 3\equiv 5 \pmod{8}.$$

我們再观察古代的大衍求一术是如何求乘率的.由前面知道,經过輾轉累减一直到余数 $r_n=1$ 为止.也就是說,q_n 是 $\frac{B}{A}$ 所对应的連分数的末了第二个部分分母. 又因为 r_n 留在左边一列, n 就一定是奇数. 显然,$(-1)^{n+1}=1$. 按照剛才的公式可知:

$$\alpha\equiv Q_n \pmod{A}.$$

如果把 Q_n 的求法与大衍求一术中寄数 k_n 的求法进行比較, 很容易看到: $Q_n=k_n$.

(当然,求反乘率也可以在連分数的性質中得到解釋.)

因此說,古代的大衍求一术与用連分数来求乘率,在理論上是完全一致的. 而大衍求一术在方法上更巧妙些(它在求出部分分母的同时,即算出了对应的近似分数的分母).

我們可以为我国在 13 世紀数学上已有这样的成就而感到自豪.

对于求乘率,也可利用如下的定理(叫做欧拉法):

設 A、B 为两互質的整数.那末同余式

$$\alpha B\equiv 1 \pmod{A} \qquad \text{(I)}$$

的解是:

$$\alpha\equiv B^{\phi(A)-1} \pmod{A}.$$

証明 由欧拉定理可知:

$$B^{\phi(A)}\equiv 1 \pmod{A}.$$

也就是,

$$(B^{\phi(A)-1})\cdot B\equiv 1 \pmod{A}.$$

因此(I)的解是: $\alpha\equiv B^{\phi(A)-1} \pmod{A}$.

例1 求 α, 使 $45\alpha\equiv 1 \pmod{8}$.

因为 $\phi(8)=4$, 所以得: $\alpha\equiv 45^3 \pmod{8}$.

又 $45^3\equiv(-3)^3\equiv 5 \pmod{8}$, 也就是說,

$$\alpha\equiv 5 \pmod{8}.$$

例2 求 α, 使 $35\alpha\equiv 1 \pmod{3}$.

因为 $\phi(3)=2$, 所以得: $\alpha\equiv 35\equiv 2 \pmod 3$.

最后，我們再举一个例题，作为本章的結束.

例

解同余式組: $\begin{cases} x\equiv 1 \pmod 3, \\ x\equiv 4 \pmod 5, \\ x\equiv 2 \pmod 7, \\ x\equiv 9 \pmod{11}, \\ x\equiv 3 \pmod{13}. \end{cases}$

因为

$$3\cdot5\cdot7\cdot11\cdot13=3\cdot5005=5\cdot3003=7\cdot2145=11\cdot1365=13\cdot1155.$$

运用求乘率的方法，可得:

$$5005\cdot1\equiv1 \pmod 3,$$

$$3003\cdot2\equiv1 \pmod 5,$$

$$2145\cdot5\equiv1 \pmod 7,$$

$$1365\cdot1\equiv1 \pmod{11},$$

$$1155\cdot6\equiv1 \pmod{13}.$$

因此，$x\equiv5005+3003\cdot2\cdot4+2145\cdot5\cdot2+1365\cdot9+1155\cdot6\cdot3$

$\equiv8479 \pmod{15015}$.